21世纪高职高专规划教材

计算机应用系列

网络安全技术案例教程

归奕红　刘宁　编著



清华大学出版社

21世纪高职高专规划教材

计算机应用系列

网络安全技术案例教程

归奕红　刘　宁　编著



清华大学出版社

北　京

内容简介

本书紧密结合当前网络安全技术的发展，用通俗易懂的语言，概括介绍了网络安全知识；深入浅出地介绍了病毒、木马及恶意软件的防范、黑客攻击及其防御、防火墙、ISA Server 2006 的应用配置、IDS 与 IPS、网络安全隔离、PKI 与加密技术、Windows Server 2003 安全配置、系统安全风险评估的基础知识与应用技术。本书在编写过程中遵循理论与实践相结合的原则，提供了大量的网络安全应用实例，以使读者在掌握计算机网络安全基本原理的同时，能够胜任网络系统的安全设计与管理工作。本书每章课后均附有习题，能够帮助读者开阔思路，加深对所学内容的理解和掌握。

本书适合作为应用型本科计算机类和通信类专业的课程教材，也可作为高职高专计算机类和通信类专业及相近专业的课程教材，还可作为系统管理员、安全技术人员的培训教材或工作参考书。

图书在版编目(CIP)数据

网络安全技术案例教程/归奕红，刘宁编著. —北京：清华大学出版社，2010.2
(21 世纪高职高专规划教材. 计算机应用系列)
ISBN 978-7-302-21877-7

Ⅰ. ①网…　Ⅱ. ①归…②刘…　Ⅲ. ①计算机网络—安全技术—高等学校：技术学校—教材　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2009)第 242989 号

责任编辑：张龙卿
责任校对：刘　静
责任印制：

出版发行：清华大学出版社　　**地　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　销：全国新华书店
开　本：185×260　　**印　张**：24.25　　**字　数**：588 千字
版　次：2010 年 2 月第 1 版　　**印　次**：2010 年 2 月第1 次印刷
印　数：1～4000
定　价：00.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177 转 3103　　产品编号：029360-01



前　　言

随着计算机技术、现代通信技术和网络技术的发展，尤其是 Internet 的广泛应用，计算机网络与人们的工作和生活的联系越来越密切、越来越深入，同时也使网络系统的安全问题日益复杂和突出。计算机的应用使机密和财富集中于计算机，计算机网络的应用使这些机密和财富随时受到联网用户的攻击威胁。计算机病毒的肆虐、黑客的非法入侵、重要资料被破坏或丢失，都会造成网络系统的瘫痪。目前人们已开始重视来自网络内部的安全威胁。

近几年来，有关网络安全的书籍逐渐增多，本书与之相比较，其主要特色有以下三个方面：

第一，理论与案例相结合。本书尽量避免单纯的原理性介绍和复杂的算法介绍等内容，主要从构建一个安全的网络系统的实际需要出发，结合应用型本科和高职高专院校学生的特点，以及广大社会培训机构和个人的实际需要，通过大量的实用案例分析以及详细的实施步骤，培养上述人员分析问题和解决问题的能力，使其具备较强的动手和应用能力，以达到能够胜任网络系统的安全设计与管理工作的目的。

第二，增加了颇具实用价值的内容。例如，VMware Workstation 虚拟环境的搭建及应用，ISA Server 2006 的应用配置，Snort 入侵检测系统的搭建及应用，跨交换机 VLAN 的设置及应用，申请 Thawte 公司免费证书实现邮件安全技术，Windows Server 2003 安全配置及应用等。通过学习这些知识，读者可以在一台计算机上搭建一个仿真的网络环境，从而进行本书中所有安全技术项目的实践，并掌握很多在其他资料上无法获取的技术方法。

第三，技术资料前沿。计算机应用技术与网络技术的发展是非常迅速的，为了使本书尽量靠近新知识、新技术的前沿，我们参阅了大量的国内外最新资料，力争反映网络安全技术的最新发展。

本书层次清楚、概念准确、深入浅出、通俗易懂。本书的编写人员是柳州职业技术学院多年工作在教学第一线的教师，不仅具有丰富的教学经验，还长期对外进行技术服务，具有丰富的社会实践经验。书稿的实用价值也在授课及实际项目实施过程中得到了验证。

本书第 1、第 6、第 8～10 章(除 9.4、9.12 节外)及第 7.2、第 7.4～第 7.6 节由归奕红编写，第 2、第 4、第 5 章由刘宁编写，第 3 章由曾春编写，第 7.1、第 7.3、第 7.7、第 7.8 节由罗海波编写，第 9.4、第 9.12 节由陆晓希编写，全稿由归奕红和刘宁统编和审阅。参加本书编写的人员还有黄光明、谭耀坚、聂伟、韦柳凤、姚强等。

由于编者水平有限，书中难免有不妥之处，恳请专家和广大读者批评指正。编者的 E-mail地址：agneschunchun@163.com。

编　者

2009 年 9 月



目　录















第1章　网络安全概述

本章学习目标

- 了解网络的主要安全隐患。
- 了解常见的网络安全认识误区。
- 认识容灾的重要作用及其与备份的区别。
- 掌握网络安全设计原则。
- 了解国内外网络安全法律和法规。

随着计算机技术、现代通信技术和网络技术的发展，尤其是 Internet 的广泛应用，计算机网络与人们的工作和生活的联系越来越密切、越来越深入，同时也使网络系统的安全问题日益复杂和突出。计算机的应用使机密和财富集中于计算机，计算机网络的应用使这些机密和财富随时受到联网用户的攻击威胁。以各种非法手段企图渗入网络系统的“黑客”，随着网络的覆盖范围的扩大而迅速增加。

如何保障网络系统正常、有效地工作？如何保障敏感数据不被非法获取？在规划设计一个网络系统之前，应注意哪些问题？本章从网络安全考虑和网络安全设计原则方面进行详细分析。最后介绍国内外相关网络安全的法律和法规。

1.1　网络安全考虑

网络安全考虑是网络安全设计的第一步，既要全面、细致、综合地考虑各方面安全因素，了解网络面临的主要安全隐患，又要充分考虑企业的安全现状、应用需求，并走出常见的网络安全认识误区，才能有效地进行网络安全设计。

1.1.1　网络的主要安全隐患

网络的安全隐患主要体现在下列四个方面。

1. 病毒、木马和恶意软件的入侵

病毒、木马和恶意软件通过 Internet 进行的传播给上网用户带来极大的危害，使用户的系统被破坏，敏感数据被篡改或丢失，用户账号和口令被泄露，已经成为危及全球软件用户



的一大公害。

2. 黑客的攻击

Internet是一个开放的网络，黑客(Hacker)会利用网络系统自身存在的安全漏洞，通过使用网络命令和专用软件进入网络中的计算机系统，窃取或破坏机密数据，使系统功能受损甚至瘫痪。

3. 网上传输数据的不安全性

Internet的数据传输基于TCP/IP通信协议，该协议缺乏使传输过程中的信息不被窃取的安全措施；另外，通信业务多数使用UNIX操作系统来支持，UNIX操作系统中明显存在的安全脆弱性问题会直接影响安全服务。例如，电子邮件存在着被拆看、误投和伪造的可能性。

4. 非授权的访问

随着企业网络规模的不断扩大，企业存储系统上的敏感数据越来越多，非授权的访问往往会给企业造成难以弥补和无法估量的损失。

针对上述主要安全隐患，应采取如下应对措施：安装专业的网络版病毒防护系统；及时安装系统安全补丁，堵住系统本身的安全漏洞；对系统内存储的敏感数据进行加密保护；对于网上传输的数据采用数字签名技术；加强企业内部网络的安全管理，实行“最小权限”原则；有条件的用户还可以安装入侵检测(IDS)和入侵防御(IPS)系统；可以配置网络安全隔离系统，对内、外网络进行安全隔离。

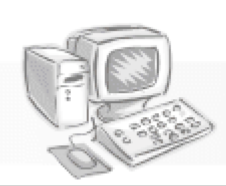
1.1.2 常见的网络安全认识误区

随着互联网技术和应用的快速发展，网络安全威胁的来源越来越复杂，手段层出不穷，网络安全产品的种类也越来越多，导致人们在认识上存在一些常见的误区，即使是网络管理员也无法全面认识和选择这些产品及对应的安全技术，给网络安全策略的制定带来漏洞。目前网络中常见的安全认识误区有如下几个方面。

1. 安装防火墙即可保障系统的安全

防火墙是网络安全的重要机制，其主要用途是根据所设定的规则，过滤掉存在安全风险的通信数据包，如黑客攻击类的端口扫描数据包、Ping测试包和拒绝服务类数据包等。但是，入侵者可以绕过防火墙进行攻击。防火墙不能防止来自网络内部的袭击，实际上将近65%的攻击都来自网络内部。防火墙不能过滤掉计算机病毒、木马及恶意软件等的入侵和感染。所以，防火墙只是整个企业安全防御系统中的一个重要环境，并不是全部。

在2001年9月第一次出现的Nimda病毒，不但通过电子邮件进行传播，而且通过在服务器上共享的文件进行传播，它还利用了包含有Java脚本代码的Web页。它传播和造成损失的速度比以往的任何病毒都要快。Nimda病毒比其他病毒都更能说明多层安全措施的必要性，仅仅安装防火墙是远远不够的。



2. 安装杀毒软件即可预防所有病毒的入侵

任何一款杀毒软件都不能保证能完全查杀所有已知和未知的病毒,何况杀毒软件查杀某一病毒的能力总是滞后于该病毒的出现,所以当病毒库代码还没有来得及更新之前,这些新病毒仍可能成功入侵系统。

3. 不上互联网就不会感染病毒

病毒主要是通过互联网进行传播,但并不意味着不上互联网就不会感染病毒,病毒还可以通过U盘、移动硬盘和光盘等存储媒介传播。局域网中只要有一台计算机感染了病毒,则整个局域网都很可能受到感染。

4. 文件属性设置为只读就可以拒绝病毒

病毒或黑客程序可以修改文件属性,因此,设置只读并不能有效防毒。为了防止病毒感染,可以采取对文件夹或文件进行数据加密的方法,这样病毒就无法感染其中的文件了。

5. 在每台计算机中安装单机版杀毒软件与安装网络版杀毒软件等效

有些企业为了节省成本,购买单机版杀毒软件,他们认为在每台计算机上安装这些单机版杀毒软件与安装网络版杀毒软件等效。这种认识是非常错误的。网络版杀毒系统不等于在每台机器上安装杀毒软件,它的核心是集中的网络防毒系统管理。网络版杀毒软件可以在一台服务器上通过安全中心控制整个网络的客户端杀毒软件进行同步病毒查杀、软件系统升级,同时架空整个网络的病毒,使病毒无处藏身。而单机版杀毒软件只能孤军作战,很难实现整个网络同步进行病毒查杀和软件升级、更新。

此外,网络版杀毒软件可以在一台服务器上进行统一的病毒防护策略部署。这对于整个网络的管理非常方便,而单机版杀毒软件是不可能做到的。如果网络规模比较大,要为每台计算机单独进行防护配置几乎是不可能的。

6. 安装多个杀毒和防火墙软件可以使系统更安全

这种观点并不是完全错误,但很不现实。不同的杀毒软件和防火墙软件的防毒和防攻击能力不一样,实验证明,使用某个杀毒软件对系统进行全面查杀后,再用另外的杀毒软件还能查出一些病毒、木马和恶意软件。但是在企业网络中,如果安装多个杀毒和防火墙软件,不仅增加了大量的成本,还会严重影响网络性能,何况大多数杀毒和防火墙软件的绝大部分功能是相同的,如此做法所获得的好处不大。此外,不同品牌的杀毒软件和防火墙软件还可能存在冲突,甚至根本不能安装或运行。

7. 网络安全威胁主要来源于外部网络

《信息周刊》研究部2008年的调查显示,60%以上的网络威胁和攻击来自网络内部,如未经授权的雇员对文件或数据的访问、带有公司数据的可移动设备遗失或失窃等。但是这一点却并没有引起企业足够的重视,许多网络管理员和企业领导还一直认为,只要做好对外部网络攻击的防范就可以保障网络安全了。这种观点对于目前的网络安全形势来说是非常



危险的。

8. 只要及时做数据备份即可保证数据安全

数据备份的任务和意义在于，当灾难（如自然灾害、病毒侵入、人为破坏等）发生后，通过备份的数据能完整、快速、简捷、可靠地恢复原有系统。但是，认为只要及时做好数据备份就可以高枕无忧是错误的。试想一下，如果黑客取得了合法用户账户，不断在网络中进行破坏行动，这样的恶性数据备份有什么用呢？难道只能每天把系统、数据恢复到原始状态吗？数据备份只是企业网络安全的最后一道防线，在它前面必须部署一系列的防护措施，才能保证企业网络的安全。

9. 投资太大，等需要时再建设

建设一套完备的安全机制来保护企业网络系统，其投资是比较大的，因此，许多企业（尤其是小型企业）不愿意一次性作这样的投资，而是选择最简单的、成本最低的防护方法（如安装杀毒软件），以后则“头痛医头，脚痛医脚”，根据“需要”建设相应的安全机制。这样做的后果往往是企业内部许多重要数据丢失，机密文件泄露，网络系统不能正常运作，严重的可以导致企业破产，其经济损失远远大于建设一套完备的安全防护机制。

1.1.3 备份与容灾

尽管人们十分小心，但是自然灾害无法躲避。1993 年，美国世贸中心大楼发生爆炸，一年后，能回到世贸大楼工作的公司由 350 家变成了 150 家，有 200 家公司由于无法取回原有重要信息而倒闭。据 IDC（Internet Data Center，互联网数据中心）的统计数字表明，美国在 2000 年以前的 10 年间发生过灾难的公司中，有 55％当时倒闭，剩下的 45％中，也有 29％因为数据丢失在两年之内倒闭，生存下来的仅占 16％。GartnerGroup 的数据也表明，在经历大型灾难而导致系统停运的公司中，有 2/5 再也没有恢复运营，剩下的公司中也有 1/3 在两年内破产。

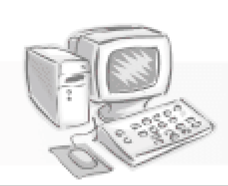
根据有关机构统计，对关键业务运行要求最高的银行业，每次计算机系统宕机导致的损失平均为 1000 万美元，同时还会导致对公司声誉无法估量的无形资产损失，而采取灾难恢复方案总共花费平均只有 100 万美元。

因此，企业需要一套完整的数据备份及容灾解决方案，以确保业务数据能有效安全地备份和恢复，减少企业的损失。

1. 备份

备份指用户为应用系统产生的重要数据制作一份或者多份副本，以增强数据的安全性。备份不是简单的复制，备份文件远远小于原文件，它用一种安全的形式保存，不容易被破坏，且能以恢复的形式还原所有数据。

在备份的几大技术中，硬盘存储、光存储、磁带存储都已经实现大容量，都可以作为备份方案的选择。然而，考虑到存储介质单位成本的问题，只有磁带技术才真正适合数据备份。



2. 容灾

容灾是一项系统工程，而不仅仅是技术。容灾系统是指在相隔较远的异地建立两套或多套功能相同的 IT 系统，相互之间可以进行健康状态监视和功能切换，当一处系统因意外(如火灾、地震等)停止工作时，整个应用系统可以切换到另一处，使得该系统功能可以保持不间断的工作。

1) 容灾的分类

按容灾对系统的保护程度可以划分为数据容灾和应用容灾。

(1) 数据容灾。数据容灾指建立一个异地的数据系统，该系统是本地关键应用数据的一个实时复制。采用的主要技术是数据备份和数据复制技术，其技术实现方式可以分为同步传输方式和异步传输方式。

(2) 应用容灾。应用容灾指在数据容灾的基础上，在异地建立一套完整的与本地生产系统相当的备份应用系统(可以是互为备份)，当灾难发生时，远程系统迅速接管业务运行。建立这样的系统比较复杂，不仅需要一份可用的数据复制，还要有包括网络、主机、应用、甚至 IP 等资源，以及各资源之间的良好协调。主要的技术包括负载均衡、集群技术。

对于业务应用繁多、并且系统需要保持 7×24 小时连续运行的企业来说，显然需要高级别的应用容灾系统来满足他们的需求。

数据容灾是抗御灾难的保障，而应用容灾则是容灾系统建设的目标。

2) 容灾的关键技术

建立容灾系统涉及多种技术，如：SAN 或 NAS 技术、远程镜像技术、基于 IP 的 SAN 的互联技术、快照技术等。下面重点介绍远程镜像技术、快照技术和互联技术。

(1) 远程镜像技术。远程镜像又叫远程复制，是容灾备份的核心技术，同时也是保持远程数据同步和实现灾难恢复的基础。远程镜像按请求镜像的主机是否需要远程镜像站点的确认信息，又可分为同步远程镜像和异步远程镜像。

同步远程镜像将本地数据以完全同步的方式复制到异地，每一个本地的 I/O 事务均需等待远程复制的完成确认信息才能释放，对本地系统性能影响较大。异步远程镜像的数据复制是以后台同步的方式进行的，这使本地系统性能受到的影响很小。

(2) 快照技术。远程镜像技术往往同快照技术结合起来实现远程备份，即通过镜像把数据备份到远程存储系统中，再用快照技术把远程存储系统中的信息备份到远程的磁带库、光盘库中。

快照是通过软件对要备份的磁盘子系统的数据快速扫描，建立一个要备份数据的快照逻辑单元号 LUN 和快照缓存。在快速扫描时，把备份过程中即将要修改的数据块同时快速复制到快照缓存中。快照 LUN 是一组指针，它指向快照缓存和磁盘子系统中不变的数据块(在备份过程中)。在正常业务进行的同时，利用快照 LUN 实现对原数据的一个完全的备份，可使用户在正常业务不受影响的情况下(主要指容灾备份系统)，实时提取当前在线业务数据。

(3) 互联技术。目前，出现了多种基于 IP 的 SAN(Storage Area Network，存储域网络)的远程数据容灾备份技术。它们是利用基于 IP 的 SAN 的互联协议，将主数据中心 SAN 中的信息通过现有的 TCP/IP 网络，远程复制到备援中心 SAN 中。当备援中心存储的数据量过大



时，可利用快照技术将其备份到磁带库或光盘库中。这种基于IP的SAN的远程容灾备份，可以跨越LAN（Local Area Network，局域网）、MAN（Metropolitan Area Network，城域网）和WAN（Wide Area Network，广域网），成本低、可扩展性好，具有广阔的发展前景。

3）衡量容灾备份的两个技术指标

（1）RPO（Recovery Point Objective，数据恢复点目标）：指业务系统所能容忍的数据丢失量。

（2）RTO（Recovery Time Objective，恢复时间目标）：指所能容忍的业务停止服务的最长时间，也就是从灾难发生到业务系统恢复服务功能所需要的最短时间周期。

RPO针对的是数据丢失，而RTO针对的是服务丢失。RTO和RPO必须在进行风险分析和业务影响分析后根据不同的业务需求确定，对于不同企业的同一种业务，RTO和RPO的需求也会有所不同。

3. 备份与容灾的联系和区别

备份与容灾是存储领域两个极其重要的部分，二者有着紧密的联系。备份与容灾都有数据保护作用，备份是存储领域的基础，在一个完整的容灾方案中必然包括备份的部分。同时，备份还是容灾方案的有效补充，因为容灾方案中的数据始终在线，因此存储有完全被破坏的可能，而备份提供了额外的一条防线，即使在线数据丢失也可以从备份数据中恢复。

但是，备份与容灾也有本质的区别，如表1-1所示。

表1-1　备份与容灾的区别

区　别	备　　份	容　　灾
从定义上区别	备份指用户为应用系统产生的重要数据制作一份或者多份副本，以增强数据的安全性	容灾指在相隔较远的异地建立两套或多套功能相同的IT系统，当一处系统因意外停止工作时，整个应用系统可以切换到另一处来保持正常工作
从关注的对象上区别	备份关注数据的安全，可以把备份称作是“数据保护”	容灾关注业务应用的安全，可以把容灾称作“业务应用保护”
从表现形式上区别	通过备份软件并使用磁带（或磁盘、光盘等）对数据进行复制	通过高可用方案将两个站点连接起来
从性能、成本上区别	备份大多采用磁带方式，性能低，成本也低	容灾采用磁盘方式进行数据保护，数据随时在线，性能高，成本也高

1.2　网络安全设计原则

1. 综合性、整体性原则

该原则要求进行网络安全策略设计时要全面考虑各种安全因素，确保在网络发生被攻击、破坏事件后，能尽可能快速地恢复网络信息中心的服务，减少损失。因此，网络安全系统应该包括安全防护机制、安全检测机制和安全恢复机制。安全防护机制是根据具体系统存在的各种安全威胁采取的相应的防护措施，避免非法攻击；安全检测机制是检测系统的运行情况，及时发现并制止对系统进行的各种攻击；安全恢复机制是在安全防护机制失效的情况



下，能尽量完整、快速地恢复系统，减少攻击的破坏程度。

2. 需求、风险、代价平衡的原则

任何网络系统都不可能做到绝对的安全，因为新的威胁会不断地涌现。安全是一个动态的过程，所以安全体系设计要正确处理需求、风险与代价的关系。网络系统是否达到安全目标，没有统一的标准，只能取决于用户的需求及其应用环境，具体取决于系统的规模和范围、系统的性质和信息的重要程度。只要将安全风险降低到一个可接受的程度，使用户和决策者可以接受剩余的风险即可。

3. 一致性原则

安全防护系统是一个庞大的系统工程，其安全体系的设计必须遵循一系列的标准，只有这样才能确保各个分系统的一致性，使整个系统能实现安全通信、信息共享。

4. 等级性原则

等级性原则是指安全层次和安全级别。良好的信息安全系统必然是分为不同等级的，包括对信息保密程度分级，对用户操作权限分级，对网络安全程度分级（安全子网和安全区域），对系统实现结构的分级（应用层、网络层、数据链路层等），从而针对不同级别的安全对象提供全面、可选的安全算法和安全体制，以满足网络中不同层次的各种实际需求。

5. 易操作性原则

安全措施的执行是靠人来完成的，如果措施过于复杂，对人的要求太高，造成执行的困难，其本身就降低了安全性。此外，安全措施的采用不能影响系统的正常运行。

6. 分步实施原则

由于政策规定、服务需求的不明朗，以及环境、条件、时间的变化，攻击手段的进步，安全防护不可能一步到位，可在一个比较全面的安全规划下，根据网络的实际需要，先建立基本的安全体系，保证基本的、必需的安全性。随着网络规模的扩大、应用的增加和网络复杂程度的变化，网络系统的漏洞也会逐步出现，此时应及时调整网络安全设计方案，增强安全防护力度，保障整个网络系统的安全。

7. 技术与管理相结合原则

安全攻击的手段在不断更新，来源也越来越复杂，不仅有来自外部网络的攻击，还有大量来自内部网络的攻击，涉及人、技术、操作和管理等多方面因素。单靠技术或单靠管理都不可能实现安全防护，必须将各种安全技术、人员培训、管理机制、法律与法规建设等结合起来，才能较好地保障企业网络系统的安全。

1.3　网络安全的法律和法规

计算机犯罪是一种高技术犯罪活动，也是未来社会的主要犯罪形式之一，因此，面对日益严重的计算机犯罪，必须建立相关的法律、法规进行约束：通过建立国际、国内和地方计



算机信息安全法来减少计算机犯罪案(如盗窃网络设施、非法侵入网络来破坏和盗窃信息资源、故意制造病毒破坏网络系统等)的发生。由于法律具有强制性、规范性、公正性、威慑性和权威性,因此它在很多方面具有不可替代的作用。制定并实施计算机信息安全法律,加强对计算机网络安全的宏观控制,对危害计算机网络安全的行为进行制裁,为网络信息系统提供一个良好的社会环境是十分必要的。

1.3.1 国外的相关法律和法规

在国际上,由于发达国家的计算机应用已非常普及,因此,其计算机安全立法工作也早已进行。1987 年出现了世界上第 1 部计算机犯罪法——佛罗里达计算机犯罪法,它首次将计算机犯罪定为侵犯知识产权罪。随后,各发达国家针对计算机犯罪的刑事责任的追究,纷纷修改刑法,增加计算机犯罪的惩治条款,或单独立法,对计算机犯罪的定罪、量刑所产生的威慑力,可使有犯罪企图的人产生畏惧心理,从而减少犯罪的可能,保持社会的安定。

这些法规认定的违法行为的内容大体相似,主要有以下几个方面:

(1) 窃取国家、科学、公众、私人机密。

(2) 有诈骗企图,非法更改、伪造、删除、破坏数据资料或向资料中掺假。

(3) 擅自故意非法操作计算机、网络,造成合法用户无法用机。

(4) 破坏计算机系统及系统硬件设备、数据。

法规的具体内容可以参考以下美国联邦计算机犯罪法和英国计算机滥用法的有关规定。

1. 美国联邦计算机犯罪法(《计算机诈骗和滥用法》)

该法律规定,具有以下犯罪行为的,分别处以罚款或者处十年以下监禁和五年以下监禁。

(1) 未经授权或越权访问计算机,并以此手段获取美国政府为保护国防或外交关系的利益而防止非法泄露的信息,或者获取 1954 年原子能法第 10 章规定的数据,而且有理由认为他们获取这类信息并加以利用,会损害美国利益或有利于他国利益。

(2) 闯入计算机系统获取金融机构、信用卡发行机构或包括顾客信用报告文件中的有关财务记录信息。正当信用报告法(Fair Credit Reporting Act)对此作出了规定。

(3) 未经允许或越权闯入由政府控制或影响政府应用的计算机系统。

(4) 闯入与联邦利益有关的计算机系统,并企图诈骗获取任何除应用此计算机以外的有价值的东西。

(5) 未经授权,故意访问涉及联邦利益的计算机,并有一个以上证据说明其有更改、损害、毁灭这种计算机中的信息的行为,或者阻碍对这种计算机或信息的合法使用,以至于在任何一年内造成损失总计 1000 美元。还包括篡改或损害医疗检查、诊断、治疗、保健数据。

(6) 故意和有预谋地对美国州际、外贸或者政府使用的计算机的口令进行诈骗。

2. 英国计算机滥用法

该法律规定计算机滥用罪行如下:

(1) 未经授权存取计算机资料,判处六个月以下监禁或者处以罚款标准第五级以下的罚款数额,或者两项并处。

（2）企图进行进一步犯罪活动的未经授权的存取。

一个人在第一条的前提下有企图并实施犯罪行为的，就构成了犯罪，具体包括：实施本条规定的罪行；本人或促使他人进行犯罪，并且企图实施的行为属于本条规定的进一步的犯罪。

对进一步的犯罪，处以六个月以下监禁或者处以法定最高标准以下罚款数额，或者两项并处。

未经授权更改计算机资料包括下列行为。

① 未经授权变更任何计算机的内容。

② 犯罪行为发生时有一定的意图和意识：损害计算机的运行；妨碍、阻止正常存取计算机中的程序或数据；损害程序的运行或数据的可靠性。

以上行为可处以六个月以下监禁或处以法定最高标准以下的罚款数额，或两项并处。经诉讼程序的判决，可判五年以下监禁或者罚款，或者两项并处。

不同形式的法律，如《计算机安全法》、《信息自由法》、《伪造访问设备和计算机欺骗与滥用法》、《数据保护法》、《计算机犯罪法》、《计算机软件保护法》、《电子资金转账法——保密法》、《个人隐私法》等在一些国家均已出台，一些国家还将计算机犯罪与刑法、民法联系在一起，修改有关条款并颁布实施，收到了较好的效果。

1.3.2　我国的相关法律和法规

我国国务院、公安部等有关单位从1994年起制定并发布了《中华人民共和国计算机信息系统安全保护条例》等一系列计算机网络安全方面的法规。这些法规主要涉及信息系统安全保护、国际联网管理、商用密码管理、计算机病毒防治、安全产品检测与销售五个方面。下面做简单介绍。

1. 计算机网络安全及信息系统安全保护

（1）1991年，国务院第83次常委会议通过《计算机软件保护条例》。

（2）国务院于1994年2月发布《中华人民共和国计算机信息系统安全保护条例》。

（3）1997年10月，我国第一次在修订刑法时增加了计算机犯罪的罪名。

（4）2000年12月，第九届全国人大常委会通过了《全国人大常委会关于维护互联网安全的决定》。

（5）后来发布了中华人民共和国国家军用标准，包括：《指挥自动化计算机网络安全要求》、《军队通用计算机系统使用安全要求》。

（6）中国人民银行令[2001]：《网上银行业务管理暂行办法》。

（7）证监信息字[1999]：《〈证券经营机构营业部信息系统技术管理规范（试行）〉技术指引》。

此外，我国还缔约或者参与了许多与计算机相关的国际性的法律和法规，如《建立世界知识产权组织公约》、《世界版权公约》、《与贸易有关的知识产权（包括假冒商品贸易）协议》等。

2. 国际联网管理

加强对计算机信息系统国际联网的管理，是保障信息系统安全的关键。因此，国务院、



公安部等单位共同制定了下面多个关于国际联网的法规。

(1) 国务院于1996年2月1日发布《中华人民共和国计算机信息网络国际联网管理暂行规定》。本规定体现了国家对国际联网实行统筹规划、统一标准、分级管理、促进发展的原则。

(2) 国务院信息化工作领导小组于1997年12月发布《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》。

(3) 公安部于1997年12月发布《计算机信息网络国际联网安全保护管理办法》,目的是加强国际联网的安全保护。

(4) 原邮电部于1996年发布《中国公用计算机 Internet 国际联网管理办法》,目的是加强对中国公用计算机(Internet Chinanet)国际联网的管理。后来又发布《计算机信息网络国际联网出入口信道管理办法》,目的是加强计算机信息网络国际联网出入口的管理。

(5) 国家保密局于2000年1月发布《计算机信息系统国际联网保密管理规定》,目的是加强国际联网的保密管理,确保国家秘密的安全。

3. 商用密码管理

国务院于1999年10月发布《商用密码管理条例》,目的是加强商用密码管理,保护信息安全,保护公民和组织的合法权益,维护国家的安全和利益。

4. 计算机病毒防治

1989年,公安部发布了《计算机病毒控制规定(草案)》。2000年4月,公安部又发布了《计算机病毒防治管理办法》,目的是加强对计算机病毒的预防和治理,保护计算机信息系统安全。

5. 安全产品检测与销售

公安部于1997年12月发布《计算机信息系统安全专用产品检测和销售许可证管理办法》,目的是加强计算机信息系统安全专用产品的管理,保证安全专用产品的安全功能,维护计算机信息系统的安全。

1.4 习　　题

1. 网络的主要安全隐患有哪些方面?
2. 有哪些常见的网络安全认识误区?
3. 什么是容灾? 简述容灾的重要作用及其关键技术。
4. 简述备份与容灾的关系。
5. 简述网络安全设计原则。
6. 国外的网络安全法律和法规认定的违法行为大致包括哪些方面?
7. 我国的网络安全法律和法规主要涉及哪几个方面?



第2章　病毒、蠕虫和木马的清除与预防

本章学习目标

- 计算机病毒的分类。
- 计算机病毒的主要特点。
- 部署企业网络防病毒系统。
- 蠕虫病毒的主要特征及通用的清除和预防方法。
- 木马的伪装、运行方式及通用的清除和预防方法。
- 流氓软件的主要特征、分类与预防方法。

计算机病毒、蠕虫和木马的入侵仍是目前主要的网络安全威胁之一，特别是近几年蠕虫日益猖獗，其危害性已经超过计算机病毒和木马。

计算机病毒是最古老、也是大家最熟悉的一种安全威胁。当然它也在随着计算机和网络技术的发展而发展，不仅病毒品种和类型更多，危害性更大，而且检测和查杀的难度也更大。

其中有一个明显的趋势就是网络类型的蠕虫（如维金、熊猫烧香蠕虫等）成为当前互联网主要的危害，而且还与木马类程序相结合，危害性明显加大。

木马也是当前的主要安全威胁之一，其危害性绝不比计算机病毒低，因为它可以窃取用户的有用信息和机密文件，同时也会影响计算机系统的运行。当前仍在肆意横行的灰鸽子就是当前木马程序的主要代表，其变种就有上万种之多。可见其查杀的难度有多大。

流氓软件（国内官方的定义为“恶意软件”。在本书中“恶意程序”指有害程序的总称）的危害也日趋明显，主要表现是侵占计算机系统资源、窃取用户信息、影响计算机系统运行，有人甚至认为它比计算机病毒更可怕。

本章全面介绍与计算机病毒、蠕虫和木马有关的基础知识，并通过具体的实用工具介绍相应的清除与预防方法。

2.1　计算机病毒

对计算机网络系统的最大威胁之一，就是计算机病毒。对计算机病毒的说法有两种，从广义上说，凡利用系统和程序的脆弱性及漏洞进行攻击的，能够引起计算机故障，破坏计算机数据的程序统称为恶意程序（rogue program），即广义上的计算机病毒。从狭义上说，计



算机病毒是指自身具有或使其他程序具有破坏系统功能、危害用户数据或其他恶意行为的一类程序。这类程序往往影响计算机使用,并能够自我复制。

计算机病毒程序可以通过修改某些程序以达到感染该程序的目的。修改操作可能包含复制病毒程序,然后去感染其他程序。典型的计算机病毒进入主机之后将驻留其中,临时控制计算机的磁盘操作系统,感染病毒后的计算机运行其他未感染的程序后,病毒的副本就会进入这些程序中。计算机病毒就这样通过无警惕性的用户的存储 U 盘或者在网络上交换文件传播开来。由于网络环境下访问其他计算机上的资源是一件非常普通的事情,这使得网络成为计算机病毒培育和传播的良好环境。

病毒程序可以做其他程序可以做的任何事情。与普通程序相比,病毒程序的唯一不同之处就在于,当宿主程序执行的时候病毒程序就会秘密执行自己的功能。一旦病毒被激活,就可以实现设计者所设计的功能,比如删除文件和程序等。

2.1.1 计算机病毒的主要特点

尽管计算机病毒的数量和种类都非常多,而且每天都可能有新的计算机病毒产生,但它们肯定存在某些共性,否则我们就不可能把它们统归于计算机病毒。因为我们已经知道,计算机病毒也是一种计算机程序文件,只不过其目的和运行方式与一般的程序不一样。当然它还具有许多正常程序所不具有的特点,综合起来表现在如下几个方面。

1. 未经授权执行

一般正常的计算机程序是由用户调用,再由系统分配资源运行的。它们的目的对用户是可见的、透明的;而病毒程序虽然也是计算机程序,但它必须隐藏在正常程序中,当用户调用正常程序时窃取到系统的控制权,先于正常程序执行,因为没有哪个人会主动运行那些明知是计算机病毒的程序,也没有哪个人会发现了计算机病毒文件而不进行清除,除非是专门从事计算机病毒研究的。计算机病毒的运行和最终目的对用户来说是未知的,且未经用户许可。

2. 隐蔽性

因为病毒是不受欢迎的,所以为了不被人发现,必须隐藏起来。为了实现这一目标,病毒程序一般是有很高编程技巧同时又短小精悍的程序,如只有几 KB(千字节)或者几十 KB,运行起来既不需要占用太多资源,也不需要多少时间,完全可以做到让人无法察觉。

病毒通常附着在正常程序或磁盘较隐蔽的地方,也有个别的以隐藏文件出现。这样就不易发觉。一般情况下,系统被病毒感染后用户感觉不到它的存在,计算机系统通常仍能正常运行,只有在其发作或是系统出现不正常反应时候用户才能觉察出来。典型的 Tiny 家族 DoS 病毒都很短小,最小的计算机病毒代码长度只有 133B。

3. 传染性

传染性是病毒的基本特征。病毒一旦侵入系统,它会搜索符合其传染条件的程序或存储媒介,确定目标后将自身代码插入其中,达到自我繁殖的目的。只要一台计算机染毒,如

不及时处理,那么病毒会在这台计算机上迅速扩散,其中的大量文件会被感染。而被感染的文件又成了新的感染源。当与其他机器进行数据交换或通过网络接触时,病毒会继续进行感染。病毒利用一切计算机通信资源进行传播,一般的传播媒介包括:可移动设备、硬盘,最主要的是计算机网络。是否具有传染性是判别一个程序是否为计算机病毒的最重要的条件。

4. 潜伏性

大部分病毒感染系统后一般不会马上发作,它可以隐藏在系统中,只有在满足其特定条件的时候才启动其破坏功能,这样它就可以被广泛地传播。潜伏性愈好,其在系统中的存在时间就会愈久,计算机病毒的传染范围就会愈大。著名的"黑色星期五"每逢13号的星期五发作,CIH病毒发作是在4月26号。在潜伏期间,不用专用检测程序一般检查不出计算机病毒程序,因此计算机病毒可以静静地躲在磁盘或磁带里,一旦条件满足就会发作。计算机病毒是依靠一定的触发条件进行发作的,不满足触发条件时,计算机病毒除了传染外不做什么破坏。一旦触发条件得到满足,有的在屏幕上显示信息、图形或特殊标识,有的则执行破坏系统的操作,如格式化磁盘、删除磁盘文件、对数据文件做加密、封锁键盘以及使系统崩溃等。

5. 破坏性

病毒一旦攻入了系统,会对系统及其应用程序产生不同程度的影响。轻者会降低计算机工作效率,占用系统资源;重者可以导致系统崩溃。按照影响的程度不同,可将病毒分为良性病毒和恶性病毒。一些恶性病毒会破坏数据文件,甚至破坏硬件设备。一些常见的破坏行为如下。

(1) 攻击系统数据区:修改或删除硬盘主引导扇区、FAT表以及文件目录等信息。
(2) 攻击文件:修改或删除系统文件。
(3) 攻击内存:占用大量内存、改变内存总量、禁止分配内存或蚕食内存等。
(4) 干扰系统运行:干扰内部命令执行、强制死机、重启等。
(5) 攻击磁盘:不写盘、写操作变读操作、写盘时丢失字节或者格式化硬盘等。
(6) 消耗系统资源:包括消耗操作系统资源和网络资源。
(7) 改动系统配置:比如CIH病毒就会修改FlashROM中的BIOS信息。
(8) 盗取、泄露信息。

6. 不可预见性

从对计算机病毒的检测方面来看,计算机病毒还有不可预见性。由于目前的软件种类极其丰富,某些正常程序也使用了类似病毒的操作,甚至借鉴了某些病毒的技术,所以使得用杀毒软件对病毒进行检测会造成较多的误报情况。而且病毒的制作技术也在随着计算机和网络技术的发展而不断地提高,新型计算机病毒所具有的某些技术或许在正常程序中都还没有实现,因此任何病毒检测技术只能处理已知病毒或小部分的未知病毒,不存在检测所有病毒的有效程序。病毒和检测技术始终呈相互激励的增长态势。



7. 病毒的生命周期

病毒的生命周期可分为如下四个阶段。

(1) 休眠阶段。在该阶段病毒不进行操作，而是等待触发，触发条件包括日期、其他程序或文件的出现、磁盘容量超过某个限度等。并不是所有的病毒都有这一阶段。

(2) 传播阶段。在这一阶段，病毒把自己的副本植入其他程序或者某个系统的磁盘区域。每一个被感染的程序将含有病毒的一个副本，并且此副本也开始向其他程序进行传播。

(3) 触发阶段。这一阶段病毒被激活以执行病毒设计者预先设计好的功能。与休眠阶段类似，病毒进入这一阶段同样需要一些系统事件的触发，还包括病毒本身复制的副本数达到某个门限值。

(4) 执行阶段。这一阶段病毒执行预设的功能。这些功能也有可能是无害的，比如仅仅是在屏幕上显示一条消息等；也可能是破坏性的，比如程序或数据文件的破坏等。

大多数病毒的作用范围都是针对某一特定的操作系统而设计的，某种操作系统的病毒对另一种操作系统是无效的，有些病毒还可能只是针对某一特定的硬件平台。因此，病毒的设计需要对特定系统的细节和弱点有深入的了解。

2.1.2 广义计算机病毒的分类

如今计算机病毒是越来越多了，每天网络上都会新增数以万计的病毒。病毒、蠕虫、木马等，都是我们日常网络生活中经常碰到的关于病毒的概念，那么，究竟病毒是怎么分类的呢？就请看看下面，按照不同的分类方法，计算机病毒大致可分类如下。

1. 一般分类方法

综合病毒本身的技术特点、攻击目标、传播方式等各个方面，一般情况下，将病毒大致分为以下几类：

(1) 传统病毒。传统病毒通过改变文件或者其他东西进行传播，通常有感染可执行文件的文件型病毒和感染引导扇区的引导型病毒。

(2) 宏病毒(Macro)。宏病毒是一种利用 Word、Excel 等的宏脚本功能进行传播的病毒。

(3) 恶意脚本(Script)。恶意脚本是一种做破坏的脚本程序。包括 HTML 脚本、批处理脚本、VB、JS 脚本等。

(4) 蠕虫(Worm)程序。蠕虫病毒是一种可以利用操作系统的漏洞、电子邮件、P2P 软件等自动传播自身的病毒。

(5) 木马(Trojan)程序。当病毒程序被激活或启动后用户无法终止其运行。广义上说，所有的网络服务程序都是木马，判定是否是木马病毒的标准不好确定，通常的标准是：在用户不知情的情况下安装，隐藏在后台，服务器端一般没有界面无法配置。

(6) 黑客(Hacker)程序。黑客程序利用网络来攻击其他计算机的网络工具，被运行或激活后就像其他正常程序一样有界面；黑客程序是用来攻击/破坏别人的计算机，对使用者本身的机器没有损害。

(7) 破坏性程序(Harm)。病毒启动后,破坏用户计算机系统,如删除文件、格式化硬盘等。常见的是 BAT 文件,也有一些是可执行文件,有一部分和恶意网页结合使用。

2. 按照病毒存在的载体分类

按照病毒的载体,一般可以分为以下几种:

(1) 文件型病毒。此类病毒以文件形式存在,是目前流行的主要形式。其中根据操作系统不同,又分很多类,如 DoS 类病毒、Windows 类病毒、Linux 类病毒等。这些病毒跟操作系统紧密相关。DoS 类病毒在 DOS 下面传播得很凶猛,但在 Windows 平台上已经很少了,最新的 Windows 64 已经不再支持 16 位程序了,这类病毒已经走到了尽头。

(2) 引导区病毒。此类病毒存放在软盘引导区、硬盘主引导区和系统引导区。由于病毒在宿主的操作系统启动前就加载到内存中,具有操作系统无关性,可以感染所有的 X86 类计算机。因此这类病毒将长期存在。

(3) 网络蠕虫病毒。以网络为载体,如一度流行的 SQL 杀手。当然,纯粹网络蠕虫病毒比较少。

(4) 混合类的病毒。病毒分类没有完全清晰的划分,很多病毒为了达到广泛传播的目的,通常采用更多的方式,如 3783 病毒,可以感染引导区、DOS 程序、Windows 程序;而 Winux 病毒则可以感染 Windows,也可以感染 Linux;大部分网络蠕虫病毒也是文件型病毒。表 2-1 是常见的计算机病毒分类。

表 2-1　常见的计算机病毒分类

病毒类型	特　征	危　害
文件型	感染 DOS 下的 COM、EXE 文件	随着 DOS 的消失已逐步消失,危害越来越小
引导性	启动 DOS 系统时,病毒被触发	随着 DOS 的消失已逐步消失,危害越来越小
宏病毒	针对 Office 的一种病毒,由 Office 的宏语言编写	只感染 Office 文档,其中以 Word 文档为主
脚本病毒	通过 IE 浏览器激活	用户浏览网页时会感染,清除较容易
蠕虫	有些采用电子邮件附件的方式发出,有些利用操作系统漏洞进行攻击	破坏文件、造成数据丢失,使系统无法正常运行,是目前危害性最大的病毒
木马	通常是病毒携带的一个附属程序	夺取计算机控制权
黑客程序	一个利用系统漏洞进行入侵的工具	通常会被计算机病毒所携带,用以进行破坏

3. 按照病毒传染的方法分类

按此分类方法病毒可分为四种类型:入侵型病毒、嵌入式病毒、外壳类病毒和病毒生产机。

入侵型病毒是通过外部媒介侵入宿主机器的;嵌入式病毒则是通过嵌入到某一正常的程序中,然后通过某一触发机制发作;外壳类病毒使用特殊算法把自己压缩到正常文件上,这样当被害者解压时即执行病毒程序;病毒生产机是可以“批量生产”出大量具有同一特征的“同族”病毒的特殊程序。这些病毒的代码长度各不相同,自我加密、解密的密钥也不同,



发作条件和现象不同，但其主体构造和原理基本相同。

4. 按照病毒自身特征分类

根据病毒自身存在的编码特征可以将计算机病毒分为两种：

（1）伴随型病毒。这一类病毒并不改变文件本身，它们根据算法产生 EXE 文件的伴随文件。

（2）变型病毒。这一类病毒使用一个复杂的算法，使自己每传播一份都具有不同的内容和长度。此类病毒通常是由一段混有无关指令的解码算法和被变化过的病毒体组成。

5. 本书对计算机病毒的分类

图 2-1 给出了计算机病毒的总体分类。这些计算机病毒可以分为两类，一类需要驻留在一个宿主程序内，不是独立的程序；另一类是可以独立存在的。前一类实质上是一些程序片段，它们必须依赖于一些实际应用程序、工具软件或系统程序才能生存，后者是一些可以由操作系统调度和运行的独立程序。

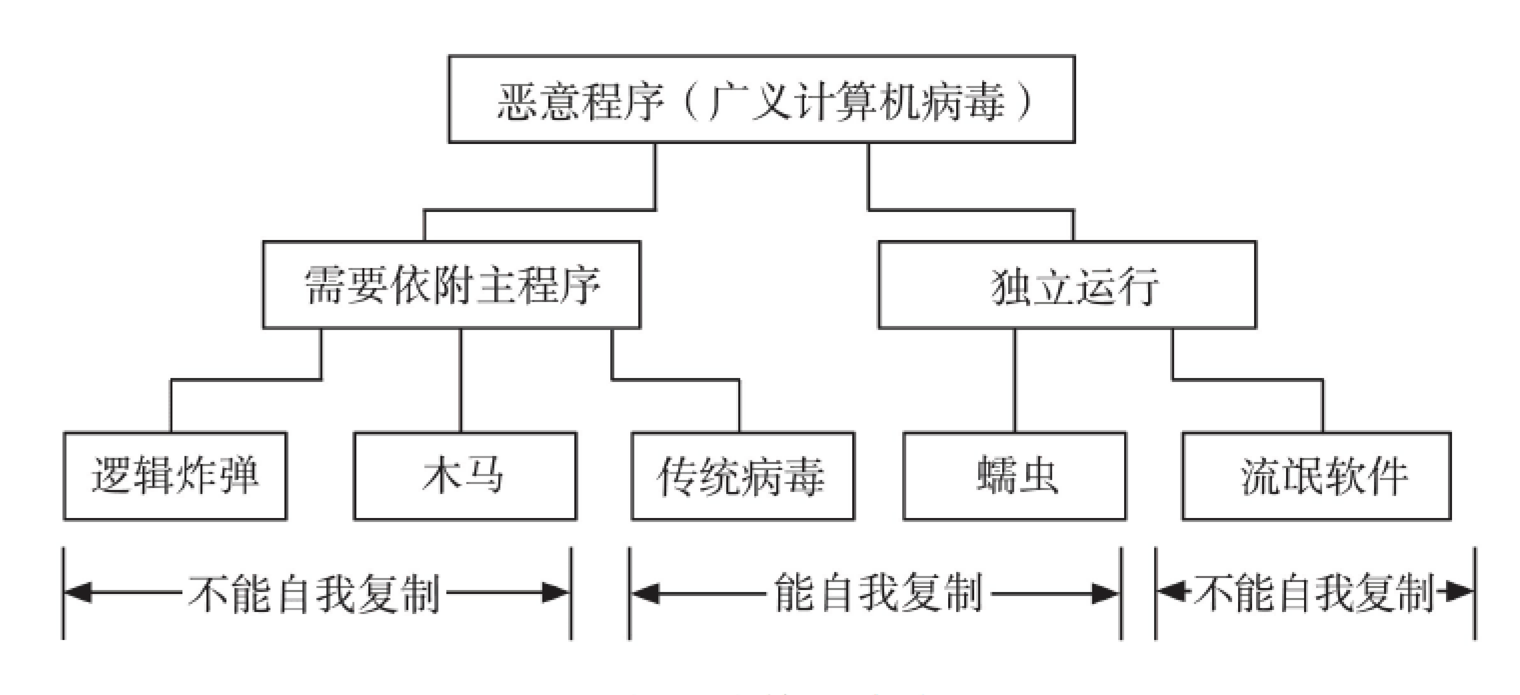


图 2-1　广义计算机病毒的分类

另外一种分类方法是将这些计算机病毒分为不可进行自身复制的和可以进行自身复制的两类。前一类在宿主程序被触发的时候执行相应程序操作，但不会进行自我复制和传播操作；后者包括程序段（传统病毒）或独立的程序（蠕虫），这些程序执行的时候将自动产生自身的一个或多个副本，这些副本在合适的时机将在本系统或其他系统内被激活。

这是本书对计算机病毒的一种分类，但这个分类不是绝对的，各种计算机病毒可以相互配合运行。例如，逻辑炸弹或木马都可能是传统病毒和蠕虫的一部分。

提示：逻辑炸弹（Logic Bomb）是出现最早的程序威胁类型之一。逻辑炸弹实际上是嵌在合法程序中的代码段，在某些条件满足的时候该炸弹将“引爆”。这些引爆逻辑炸弹的条件可能包括特定文件的出现或者消失、星期中的一个特定日子或者某特定的用户运行了一个程序等。一旦引爆，逻辑炸弹将修改、删除数据和文件，使系统停机或带来一些其他危害。例如，作为某种版权保护方案，某个应用程序有可能会在运行几次后就在硬盘中将其自身删除；某个程序员有可能希望他的程序包含某些多余的代码，以使程序运行时对某些系统产生恶意的操作。一个著名的逻辑炸弹的例子是美国的 Tim Lloyd 案例，他被指控在自己工作的 Omega Engineering 公司的网络中设置了逻辑炸弹，造成了超过一千万美元的经济损失，打乱了公司的发展计划，并导致 80 个工作人员失业。Lloyd 被判 41 个月监禁，并

罚款二百万美元。

2.1.3　计算机病毒的发展趋势

每当一种新的计算机技术广泛应用的时候，总会有相应的病毒随之出现。例如，随着微软宏技术的应用，宏病毒成了简单而又容易制作的流行病毒之一；随着 Internet 网络的普及，各种蠕虫病毒如爱虫、SirCAM 等疯狂传播。21 世纪初甚至产生了集病毒和黑客攻击于一体的病毒，如“红色代码”（CodeRed）病毒、Nimda 病毒和“冲击波”病毒等。

在网络技术飞速发展的今天，病毒的发展呈现出以下趋势：

（1）病毒与黑客技术相结合。随着网络的普及与网速的提高，使得计算机之间的远程控制越来越方便，传输文件也变得非常快捷，正因为如此，病毒与黑客技术结合以后的危害更为严重，病毒的发作往往在侵入了一台计算机后，又通过网络侵入其他的计算机。

（2）蠕虫病毒更加泛滥。其代表包括邮件病毒、网页病毒。以后，利用系统存在的漏洞而制作的病毒会越来越多，这类病毒由受到感染的计算机自动向网络中的计算机发送带毒文件，然后执行病毒程序。

（3）病毒破坏性更大。计算机病毒不再仅仅以侵占和破坏单机的资源为目的。木马病毒的传播使得病毒在发作的时候有可能自动联络病毒的创造者（如爱虫病毒），或者采取 DoS（拒绝服务）的攻击（如“红色代码”病毒）。一方面可能会导致本机机密资料的泄露；另一方面会导致一些网络服务的中止。而蠕虫病毒则会抢占有限的网络资源，造成网络堵塞（如 Nimda 病毒），如有可能，还会破坏本地的资料（如针对“9·11”恐怖事件的 Vote 病毒）。

（4）制作病毒的方法更简单。网络的普及，使得编写病毒的知识越来越容易获得。同时，各种功能强大而易学的编程工具使用户可以轻松编写一个具有极强杀伤力的病毒程序。用户通过网络甚至可以获得专门编写病毒的工具软件，只需要通过简单的操作就可以生成具有破坏性的病毒。

（5）病毒传播速度更快，传播渠道更多。目前上网用户已不再局限于收发邮件和网站浏览，此时，文件传输成为病毒传播的另一个重要途径。随着网速的提高，在数据传输时间变短的同时，病毒的传送时间会变得更加微不足道。同时，其他的网络连接方式如 ICQ、IRC（Internet Relay Chat，互联网中继聊天）也成为传播病毒的途径。

（6）病毒的检测与查杀更困难。病毒可能采用一些技术防止被查杀，如变形、对原程序加密、拦截 API（Application Programming Interface，应用程序编程接口）函数，甚至主动攻击杀毒软件等。

2.2　计算机病毒防护软件

对于计算机病毒，尽管我们可以从病毒本身的特征代码进行分析，从而找到相应的手动清除方法进行手工清除，但要真正能全面手工方式清除病毒的人少之又少。即使真能清除，那也是仅仅对个别病毒而言，这对于企业网络安全维护并没有什么实际意义。因此对于大多数用户来说，主要还是通过选用专门的杀病毒软件自动进行防护和清除。



在计算机病毒防护软件中,又可分为个人版和网络版。个人版是对单一主机进行病毒防护和清除,适用于单机的个人用户选择;而网络版是针对各个企业的不同需求,为企业网络量身定制的特定企业专用版,它对整个网络进行病毒防护和清除,适用于企业用户选择。下面分别进行介绍。

1. 个人版病毒防护软件

个人版病毒防护软件大家并不陌生,因为凡是上网的用户基本上都必须安装一款以上这类杀病毒软件。现在计算机病毒太猖獗了,不安装病毒防护软件简直不可思议,除非该用户根本不知道还有“计算机病毒”这个概念。

个人版病毒防护软件非常多,经常见到的不下10款,如国内的金山毒霸、瑞星、江民、熊猫、趋势(PC-Cillin)。目前国内的病毒防护软件的最新版基本上是2008版。国外的如俄罗斯的卡巴斯基(Kaspersky)、斯洛伐克的ESET NOD32、捷克的AVG、德国的小红伞AntiVir、罗马尼亚的BitDefender、芬兰的F-Secure AntiVirus、美国的麦咖啡(McAfee Virusscan)和诺顿(Norton AntiVirus)。这些病毒防护软件可以说是各有优、缺点,但从总体查杀病毒能力来看,国外的还是要优于国内的。根据笔者使用经验,最终认为还是像国外的卡巴斯基、NOD32和AVG不错,国内一些杀病毒软件查不到的,这些杀病毒软件却可以查出许多,而且的确是解决了许多因病毒引起的系统和应用软件故障。下面对几款经典的杀病毒软件进行简单介绍:

1) 卡巴斯基互联网安全套装8.0个人版

卡巴斯基互联网安全套装8.0个人版,是笔者试用后杀病毒和木马能力最强的病毒防护软件之一。它为计算机提供信息安全保障的组合解决方案,可使计算机免受各种网络威胁,包括:病毒、黑客攻击、垃圾邮件及间谍软件。它结合了所有卡巴斯基实验室的最新技术,针对恶意代码、网络攻击以及垃圾邮件进行防护。所有的程序组件可以无缝结合,从而避免了不必要的系统冲突,确保系统高效运行。

卡巴斯基杀病毒和木马的能力不及后面将要介绍的AVG,而且还存在许多误报现象。如对一款ADSL拨号软件运行中的Invader.exe和drwsn32.exe程序总是提示为风险软件,实际上要运行这款拨号软件就必须运行这两个程序。

2) ESET NOD32 AntiVirus 4.0

NOD32是由ESET发明设计的杀毒防毒软件。ESET于1992年创立,是斯洛伐克一个全球性的安全防范软件公司,主要为企业和个人消费者提供服务。其得奖之旗舰产品NOD32能针对已知及未知的病毒、间谍软件(Spyware)及其他对用户系统带来威胁的程序进行实时的查杀。

NOD32是由ESET(斯洛伐克一个全球性的安全防范软件公司)发明设计的近年在全球迅速崛起的一个防病毒产品。NOD32非常轻巧易用,因其惊人的侦测速度及卓越的性能,它已成为许多用户和IT专家的首选。事实上,经多家检测权威确认,NOD32在速度、精确度和各项表现上已拥有多项的全球纪录。

在速度上,NOD32保持轻巧及极快的侦察速度。根据Virus Bulletin多次的测试,NOD32的扫描速度大约比其他市场竞争者高出2~50倍,扫描速度达到70Mbps。大部分曾经使用过其他防病毒产品的用户都能感觉其不同凡响的表现能力。

在资源占用上，NOD32 整个程序的安装只占用 7～8 兆的内存空间，在安装后，大约占用 28 兆的内存空间，比其他同类产品占用的内存少约 3～5 倍。

虽然占用的空间比较小，它的性能却毫不逊色。在侦测率上，NOD32 在 Virus Bulletin 上雄踞榜首，已经连续 57 次获得 VB 100%奖项。同时，NOD32 连续 10 年在侦测上没有遗漏任何一种 ItW（In-the-Wild）计算机病毒，成为世界上唯一有此成绩的防病毒软件。

从使用经验看，NOD32 确实是一款检查速度极快、杀病毒和木马都不错的杀毒防毒软件。ESET NOD32 AntiVirus 4 是 2008 年正式上市的最新版，其主界面如图 2-2 所示。

图 2-2　ESET NOD32 AntiVirus 4 主界面

3）360 安全卫士

在这里不得不提的是奇虎公司的 360 安全卫士，主界面如图 2-3 所示。虽然 360 安全卫士只是一款完全免费的安全类上网辅助工具软件，不是真正的杀毒软件，但它不仅具有流氓软件清除功能，还具有像全面系统诊断、系统还原设置、浏览器修复、多余插件清除、插件免疫、多余软件卸载、各种历史记录清理等许多实用功能。拦截恶意钓鱼网站，防网银账户、游戏账号、QQ 账号丢失；全面查杀 9000 余款流行木马、370 款流氓软件；发布微软官方漏洞信息、修复系统漏洞，有效防止蠕虫、流氓软件通过漏洞传播。



图 2-3　360 安全卫士主界面



4) AVG Anti-Virus System 8.0

AVG Anti-Virus System 8.0 功能上相当完整,可即时侦测任何存取文件,防止计算机病毒感染;可对电子邮件和附加文件进行扫描,防止计算机病毒透过电子邮件和附加文件传播;在"病毒资料库"里面则记录了一些计算机病毒的特性和发作日期等相关资讯;"开机保护"功能可在计算机开机时侦测开机型病毒,防止开机型病毒感染。在扫毒方面,除可扫描磁盘、硬盘、光盘机外,也可对网络磁盘进行扫描。在扫描时也可只对磁盘、硬盘、光盘机上的某个目录进行扫描。可扫描文件型病毒、压缩文件型病毒(可感染 ZIP、ARJ、RAR 等压缩文件)等。在扫描时如发现文件感染病毒时,会将感染病毒的文件隔离至 AVG Virus Vault,待扫描完成后再一并解毒。

AVG Anti-Virus System 8.0 是一款优秀的计算机病毒和木马查杀软件,特别是它的木马查杀能力堪称一流。笔者曾经用多款杀毒软件做对比测试,其他杀毒软件查不出来的,AVG 却可以查出几十个病毒和木马,而且还修复了以前不能上网的问题。不过它最大的不足就是,所有查到的病毒和木马只能在整个扫描结束后统一清除,如果中途退出扫描,则不能清除任何已查到的病毒和木马,这对于大硬盘扫描的情况非常不利。

5) 趋势科技 PC-Cillin Internet Security 2008

趋势科技是我国台湾的著名杀病毒软件品牌。PC-Cillin Internet Security 2008 是目前正式上市的最新版。

趋势科技网络安全个人版集个人防火墙、防病毒、防垃圾邮件等功能于一体,最大限度地提供对桌面机的保护,但并不需要用户进行过多的操作。在用户日常使用及上网浏览时,进行"实时的安全防御监控";内置的防火墙不仅可以更方便地使用因地制宜的设定,"专业主控式个人防火墙"和"木马程序损害清除还原技术"的双重保障,还可以拒绝各类黑客程序对计算机的访问请求;趋势科技全新研发的病毒阻隔技术,包含"主动式防毒应变系统"和"病毒扫描逻辑分析技术",不仅能够精准侦测病毒藏匿与化身并予以彻底清除,还能针对特定变种病毒进行封锁与阻隔,让病毒再无可乘之机;强有力的"垃圾邮件过滤功能"能全面封锁不请自来的垃圾邮件。

趋势科技的反病毒产品具有良好的综合性优势。这款 2008 版继承了趋势科技的传统,除了在用户界面上更加美观之外,同时在功能上不断细化,使之更加人性化。

6) 小红伞 AntiVir Personal Edition 8.2

它是由来自德国著名的安全软件公司 H+BEDV 开发的。H+BEDV 是一个十分老牌的公司。它的安全产品领域覆盖了工作站、服务器、邮件站等各种网络大型终端。

这款免费的 AntiVir 专为个人用户提供,可免受计算机病毒的侵害。它可以检测并清除超过 80 000 种病毒,支持在线更新。如果想使用免费家用版,必须具备两个基本的条件:个人家庭用户与非营利性质。

AntiVir Personal Edition 所具备的防御功能包括病毒查杀、即时更新、病毒监控、病毒资料查询、日志管理、计划任务提醒等。

其查杀病毒的能力还不错,但是有时会误报,如一些 Java 脚本计数器,它也会报告为病毒,有时觉得很讨厌。

技巧:杀毒软件的选择不仅看其查杀病毒能力,还要充分考虑其所消耗的系统资源大小、所支持的操作系统(一般个人版杀病毒软件仅适用于工作站系统,如金山毒霸、卡巴斯

基等，但也有一些同时适用于工作站和服务器系统，如瑞星和 AVG 等）、误报率，以及在查杀病毒时处理方式的灵活性等方面。

另外，不建议在一台主机上安装多款杀毒软件。一般不同品牌的杀毒软件在引擎方面会相互冲突。

2. 网络版杀毒软件

尽管个人版杀毒软件的价格很便宜，而且功能也很强大，但是对于 10 个以上用户的企业网络来说，建议还是采用网络版杀毒软件。网络版杀毒软件的一个最大特点就是可以整个网络主机和服务器同步杀毒，这对于网络病毒横行的今天来说尤其重要。因为在网络中只要有一台主机感染了病毒，则可能很快（甚至是同时）在全网络主机上感染，即使其他主机已杀完了病毒。这样一来其他主机所进行的杀毒操作就前功尽弃了。

另外，网络版可以实现全网络服务器和客户端程序同步更新。还有一个管理中心控制台，可以对整个网络的服务器端和客户端程序进行集中管理，实现全网络的同步更新和杀毒。本节将介绍国内三大著名病毒防护软件的网络版杀毒软件：金山的金山毒霸网络版 5.0、江民杀毒软件 KV 网络版 2008 和瑞星杀毒软件网络版 2008。除此之外，还有国外著名的品牌，如俄罗斯的卡巴斯基（Kaspersky）、美国的 McAfee Virusscan 和 Symantec AntiVirus 等都有网络版。

1）金山毒霸网络版 5.0

金山毒霸网络版是一套专为企业级网络所设计的全网病毒防护解决方案。金山毒霸网络版采用了业界主流的 B/S 开发模式，由管理中心、控制台、系统中心、升级服务器、客户端、服务器端、特殊防毒节点 7 个模块组成了防病毒体系。它的最大特点就是体系结构配置灵活，应用部署和管理非常方便。

2）江民杀毒软件 KV 网络版 2008

江民杀毒软件 KV 网络版 2008 是为各种简单或复杂网络环境设计的计算机病毒网络防护系统。它既适用于包含若干台主机的单一网段网络，也适用于包含各种 Web 服务器、邮件服务器、应用服务器，且分布在不同城市并包含数十万台主机的超大型网络。

2008 年 2 月 28 日，国内最大的计算机反病毒软件厂商江民科技宣布，即日起启动“新春剿毒大行动”。在这次行动中推出可适用于 Windows、Linux、UNIX、FreeBSD 等多种操作系统的网络版杀毒软件“网络护卫舰——江民杀毒软件 KV 网络版 2008”，该款软件无论是从杀毒能力上还是网络管理功能上都取得了突破性的进展。在杀毒技术方面，江民杀毒软件 KV 网络版 2008 在全网统一杀毒、统一升级、统一配置和全网漏洞扫描等网络版基本功能上，独创了全网木马监控、全网检测未知病毒、全网系统启动前杀毒（BootScan）等全球领先的杀毒技术。

另外，江民杀毒软件 KV 网络版 2008 在网络管理上更取得了重大进展，产品采用了可无限分层的多级控制中心，可对大型网络进行分级，可跨地域、跨网段布防，各级控制中心对应相应层级，且每级都可实现对下级单位的统一管理。核心管理权限集中在控制中心，网管员通过账号和口令获得操作授权；提供多种客户端操作控制模式，网管员根据情况给予统一或者区别授权。同时，为了减轻网管员的劳动强度，江民杀毒软件 KV 网络版 2008 还增强了“移动安全网管”功能，网管员可以将移动控制台安装在任一移动终端中，随时随地实现对公司整个网络的智能化安全管理。



3）瑞星杀毒软件网络版 2008

瑞星杀毒软件网络版 2008 是一款应用于复杂网络结构的企业级反病毒产品。它分中小企业版、企业版和高级企业版，以及行业版等多个版本。该产品主要适用于企业服务器与客户端，支持 Windows NT/2000/XP/Server 2003、UNIX、Linux 等多种操作平台，全面满足企业整体反病毒需要。

瑞星杀毒软件网络版 2008 创立并实现了“分布处理、集中控制”技术，以系统中心、服务器、客户端、控制台为核心结构，成功地实现了远程自动安装、远程集中控管、远程病毒报警、远程卸载、远程配置、智能升级、全网查杀、日志管理、病毒溯源等功能。它将网络中的所有计算机有机地联系在一起，构筑成协调一致的立体防毒体系。

2.3 部署企业网络防病毒系统

2.3.1 Symantec NAV 10.1 企业版概述

Symantec NAV 10.1 企业版是 Symantec 最新推出的防病毒软件，用于企业内部网内的计算机防病毒，与单机版(一般个人用户只安装客户端，作用与个人版软件功能差不多)相比，企业版系统增加了网络管理功能，如病毒码的统一更新、防病毒策略的统一制定、发现病毒的网络报警等，这些网络管理功能大大减轻了网络管理员的无谓的工作量。

Symantec NAV 10.1 企业版在原有版本上做了很大的改进，删除了其中很多不实用的组件。整个光盘的大小不到 300MB，比原有老版本小了很多。

2.3.2 Symantec NAV 10.1 部署过程

按照如图 2-4 所示搭建网络，Symantec 的一级服务器安装在域控制器(建议用 Windows Server 2003 构建)ATEN-01 上，客户端可以是 Windows Server 2003、Windows XP 或 Windows 2000。

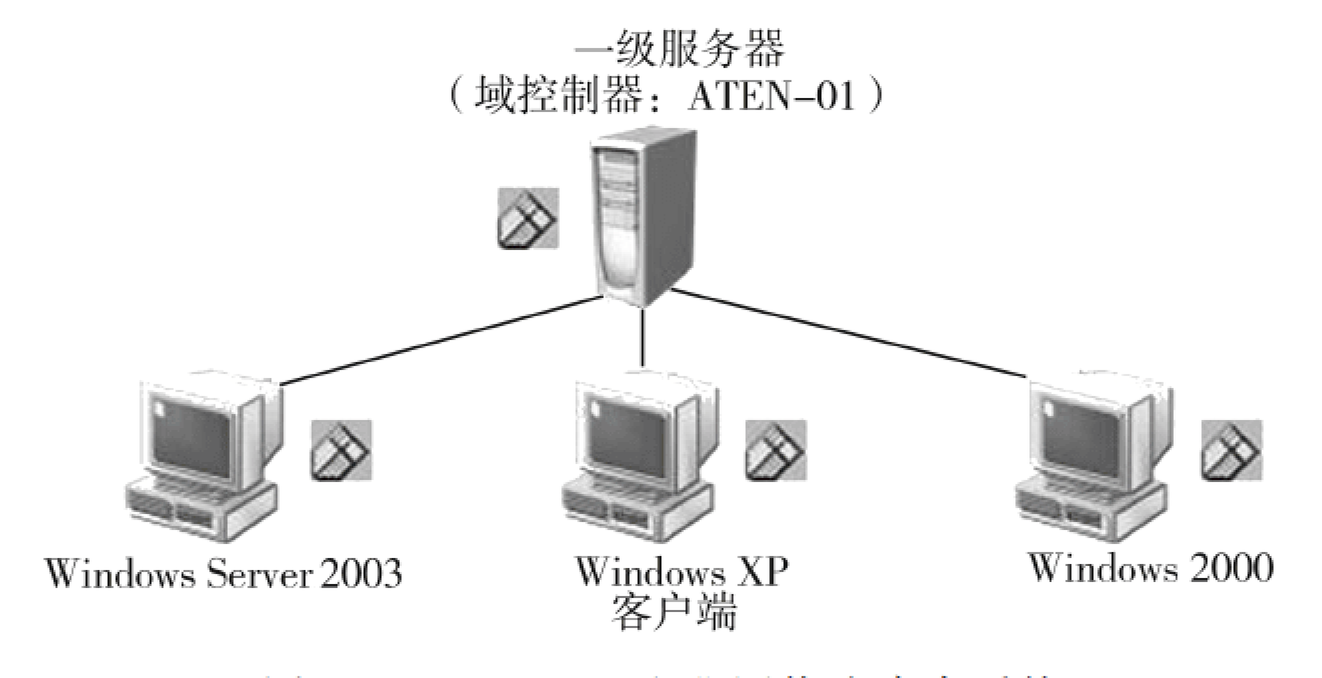


图 2-4　Symantec 企业网络防病毒系统

1. 安装 Symantec 系统中心

(1) 将 Symantec NAV 10.1 的安装光盘放入域控制器的光驱，运行光盘上 Setup.exe 程序，将出现 Symantec 的主菜单，如图 2-5 所示。





图 2-5　Symantec 主菜单

（2）选择【安装 Symantec AntiVirus】选项，将出现如图 2-6 所示的窗口，在此窗口中选择【安装 Symantec 系统中心】选项。



图 2-6　【安装 Symantec AntiVirus】菜单

（3）在出现的【授权许可协议】对话框中，选择【我接受该许可证协议中的条款】选项，单击【下一步】按钮，如图 2-7 所示。

（4）在【选择组件】对话框中选择安装的组件，如图 2-8 所示。默认可选的管理组件如下。

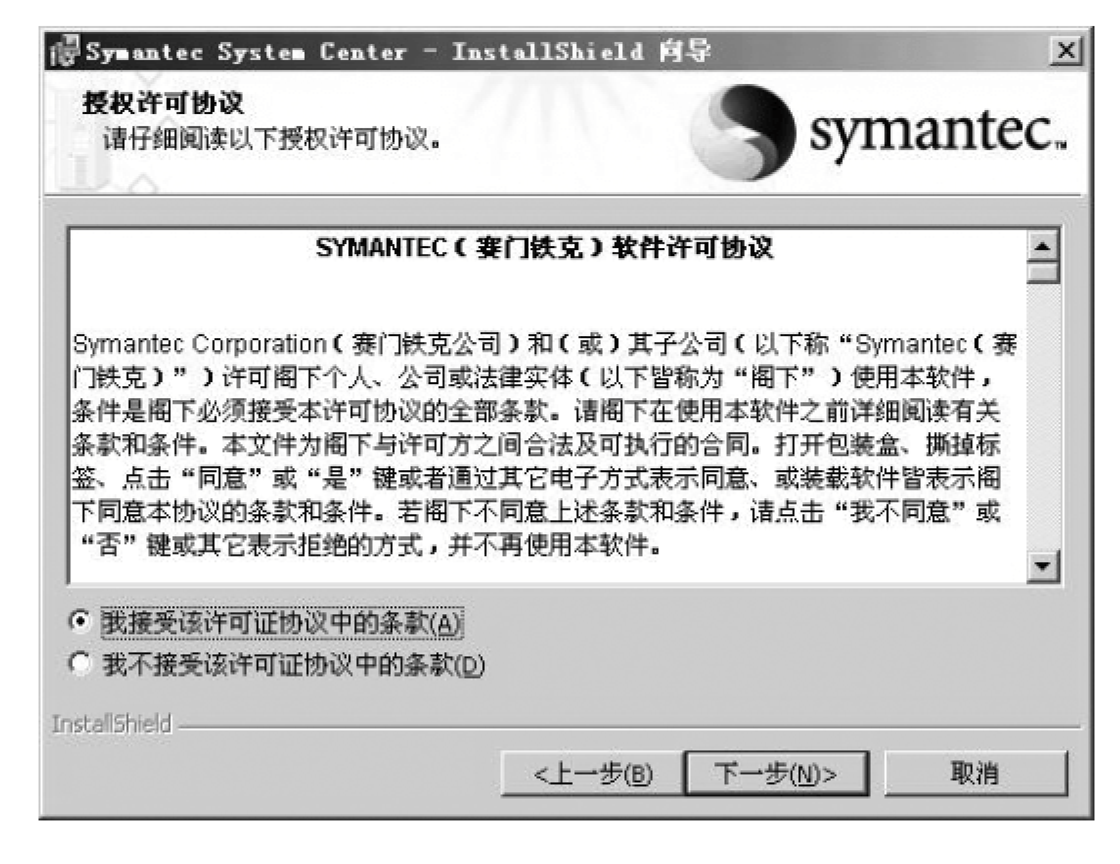


图 2-7　授权许可协议

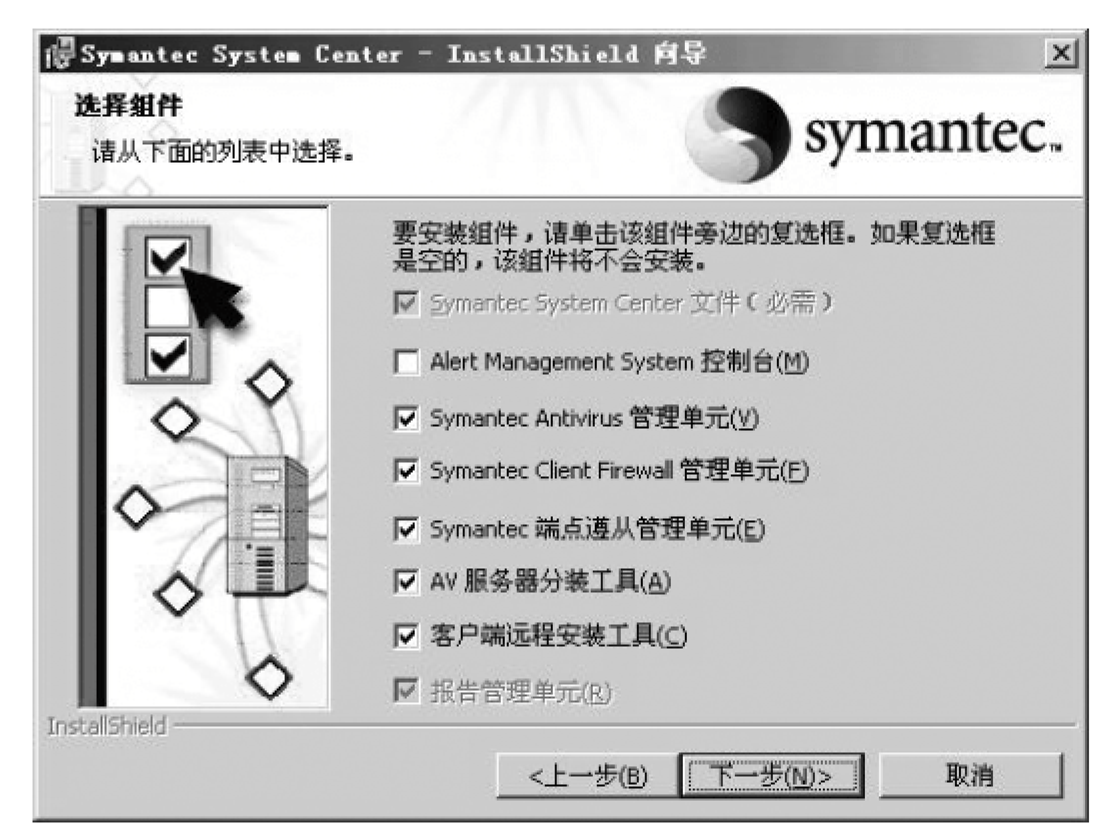


图 2-8　选择组件



① Symantec AntiVirus 管理单元：如果要集中管理病毒防护，必须安装该项对应内容。

② Symantec Client Firewall 管理单元：不是防病毒管理所必需的组件，仅适用于防火墙客户端管理。

③ AV 服务器分装工具：要将服务器安装推送到远程计算机，必须安装它。在 Symantec AntiVirus 光盘上可以找到此工具。

④ 客户端远程安装工具：要将 Symantec AntiVirus 客户端安装推送到运行受支持的 Microsoft Windows 操作系统的远程计算机上，必须安装它。在 Symantec AntiVirus 光盘上可以找到此工具。

⑤ Symantec AntiVirus 服务器：要管理运行 Symantec AntiVirus 客户端程序的联网计算机，必须安装它。它还为运行它的计算机提供病毒防护。该服务器程序允许用户将防病毒安全策略和内容更新推送到接受管理的客户端。要保护 Symantec AntiVirus 网络服务器，应安装 Symantec AntiVirus 客户端程序。

（5）在【目标文件夹】对话框中，单击【更改】按钮，可以更改程序安装的位置，如图 2-9 所示。

（6）在【准备安装程序】对话框中，单击【安装】按钮，即开始安装，如图 2-10 所示。



图 2-9　选择目标文件夹



图 2-10　准备安装程序

（7）程序安装完毕后，弹出【安装程序信息】对话框，单击【是】按钮，将重新启动计算机系统，如图 2-11 所示。

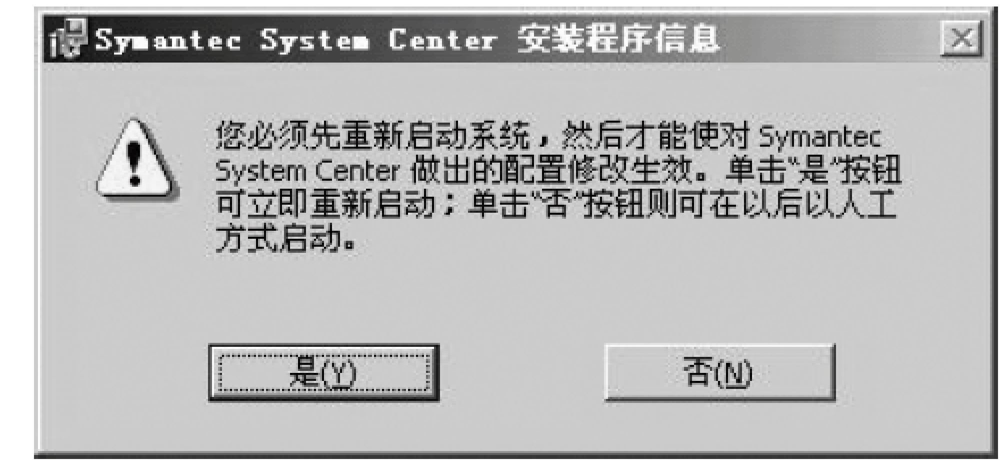


图 2-11　重新启动系统

2. 部署 Symantec 服务器

安装 Symantec 服务器有两种方法：一是在安装光盘的安装菜单中选择【安装 Symantec AntiVirus 服务器】，如图 2-12 所示；二是在 Symantec 系统中心控制台中安装。在此将介绍第二种安装方法。

（1）选择【开始】/【Symantec 系统中心控制台】命令，如图 2-13 所示。





图 2-12　安装 Symantec AntiVirus 服务器



图 2-13　选择【Symantec 系统中心控制台】命令

(2) 在打开的【Symantec 系统中心控制台】窗口中，选择【工具】/【防病毒服务器分装】命令，如图 2-14 所示。

(3) 在弹出的【欢迎】对话框中，选择【安装 Symantec AntiVirus 服务器】，然后单击【下一步】按钮，如图 2-15 所示。



图 2-14　选择【防病毒服务器分装】命令



图 2-15　【欢迎】对话框

(4) 在【许可协议】对话框中，选择【同意】单选按钮，然后单击【下一步】按钮，如图 2-16 所示。

(5) 在【选择项目】对话框中，选中【服务器程序】和【报告代理】复选框，单击【下一步】按钮，如图 2-17 所示。

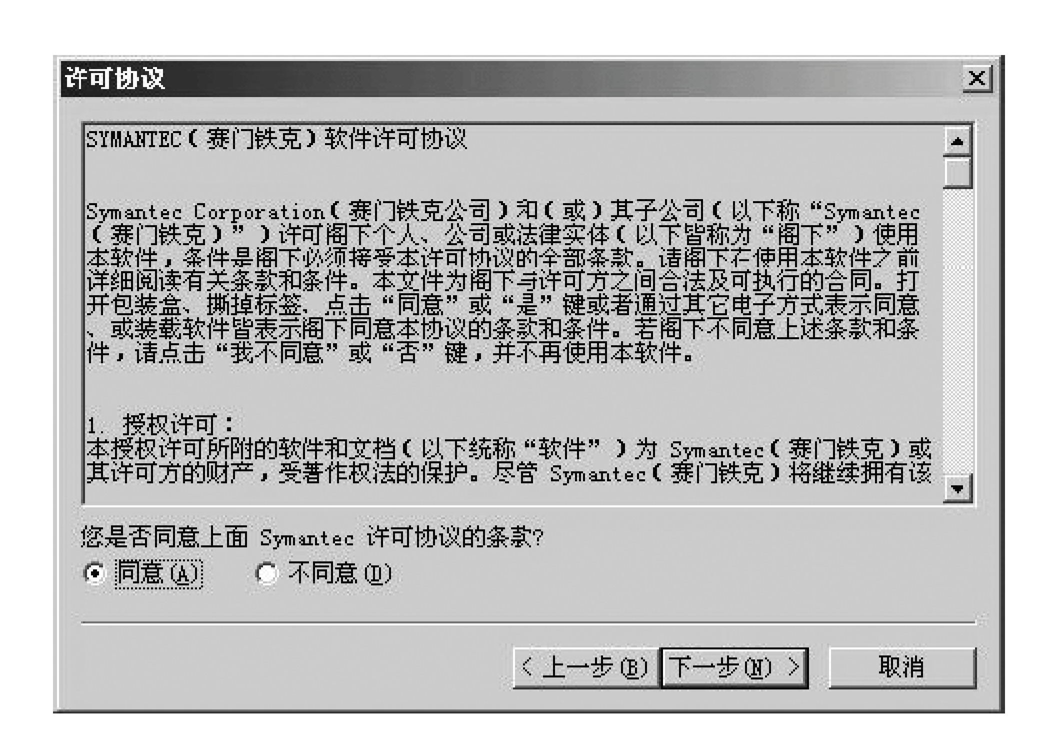


图 2-16　【许可协议】对话框



图 2-17　选择安装项目



（6）在【选择计算机】对话框左边的【网络】列表框中，选择安装 Symantec 服务器的计算机，然后单击【添加】按钮，将选择的计算机添加到右边的【目标计算机】列表框中，单击【下一步】按钮，如图 2-18 所示。

（7）在【服务器摘要】对话框中，单击【更改目录】按钮，可以更改程序安装的位置，单击【下一步】按钮，如图 2-19 所示。

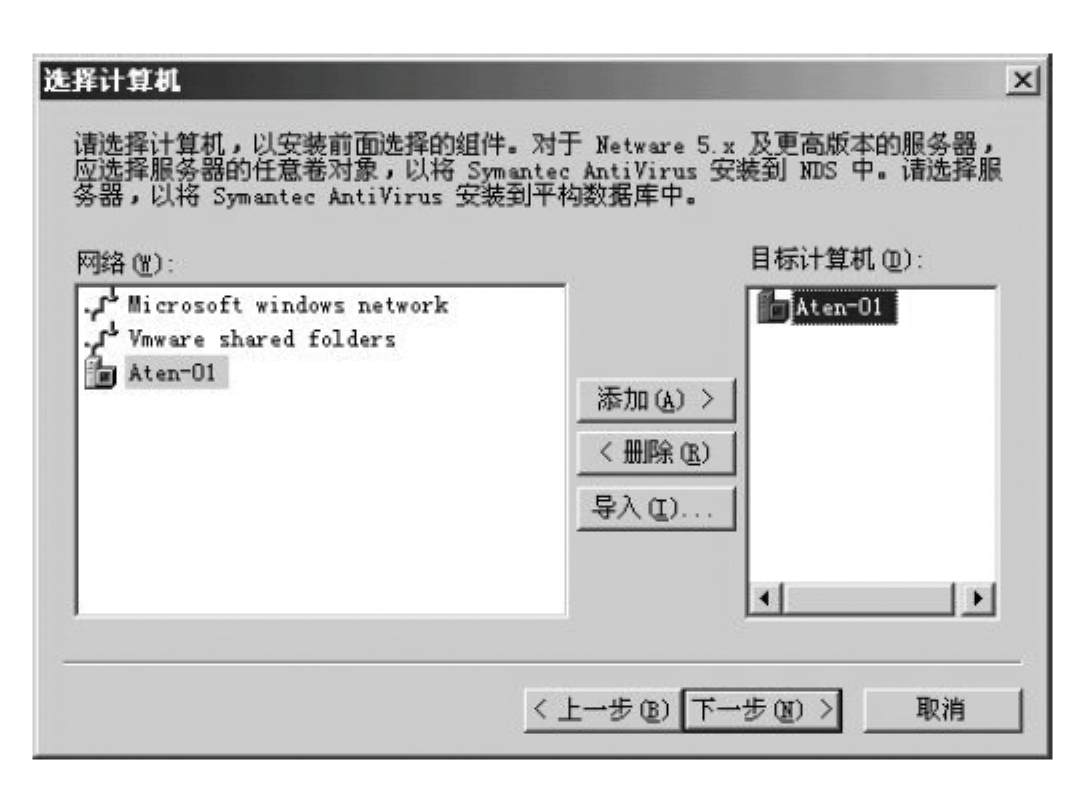


图 2-18 【选择计算机】对话框



图 2-19 选择安装路径

（8）在如图 2-20 所示的【Symantec AntiVirus 服务器组】文本框中输入服务器组的名称。

（9）在【输入服务器组的密码】对话框中，输入用户名和密码，单击【确定】按钮，如图 2-21所示。



图 2-20 服务器组名称

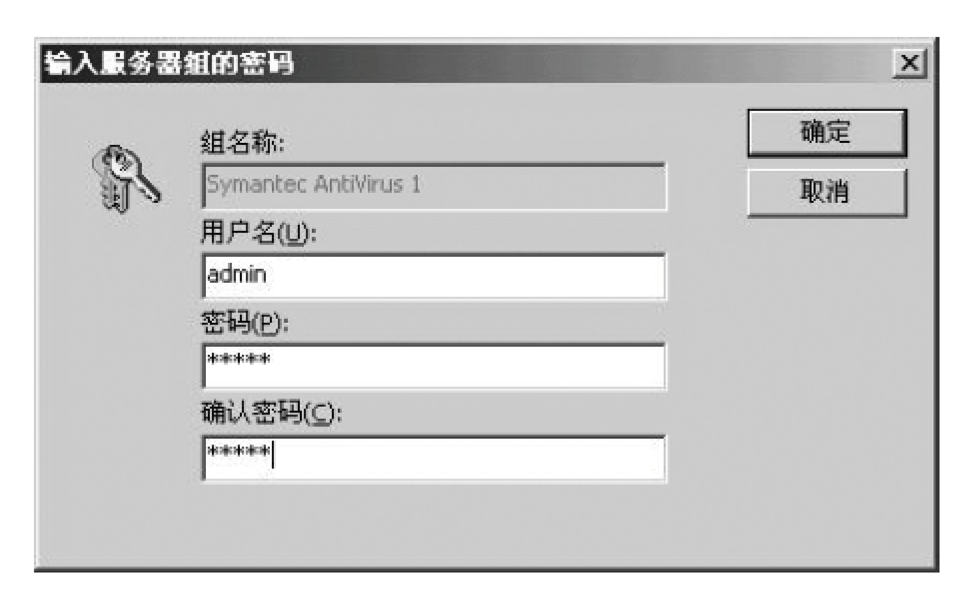


图 2-21 输入服务器组的用户名和密码

（10）在【服务器启动选项】对话框中，选择【自动启动】单选按钮，单击【下一步】按钮，如图 2-22 所示。

（11）在【使用“Symantec 系统中心”程序】对话框中，单击【下一步】按钮，如图 2-23 所示。

（12）在【安装概要】对话框中，单击【完成】按钮，如图 2-24 所示。

（13）在【安装进度】对话框中，安装完成之后，单击【关闭】按钮，如图 2-25 所示。







图 2-22　选择服务器程序的运行方式



图 2-23　提示使用“Symantec 系统中心”程序

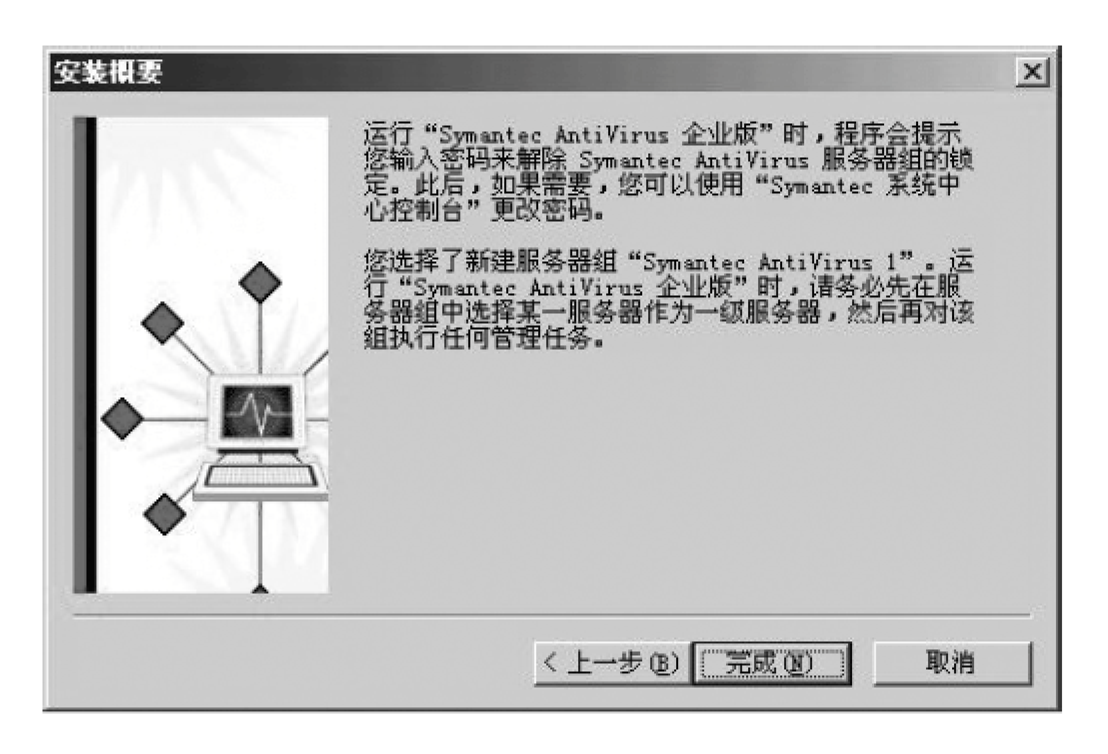


图 2-24　【安装概要】对话框

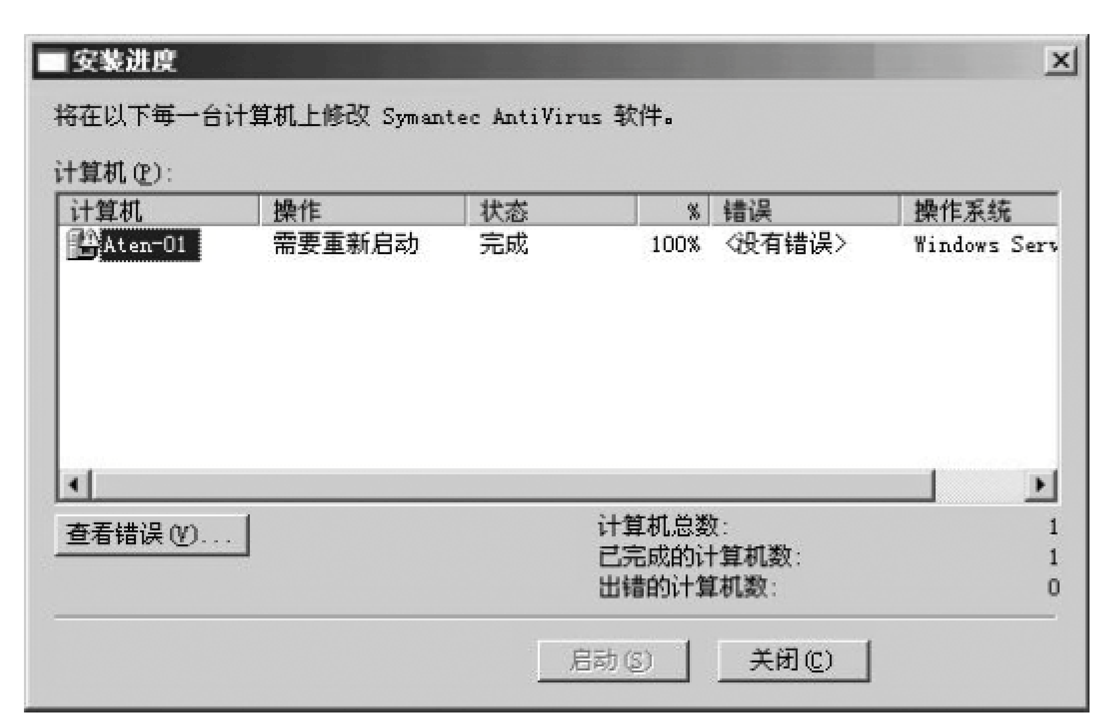


图 2-25　【安装进度】对话框

(14) 计算机系统重新启动之后，参考步骤(1)打开【Symantec 系统中心控制台】窗口。右击服务器组名称(例如 Symantec AntiVirus 1)，在弹出的菜单中选择【解除服务器组的锁定】命令，如图 2-26 所示。



图 2-26　解除服务器组的锁定



（15）在【解除服务器组的锁定】对话框中输入用户名称和密码，如果不想每次启动时都输入用户名和密码，可以选中【请记住此用户名和密码】复选框，然后单击【确定】按钮，如图 2-27 所示。

（16）在【Symantec 系统中心控制台】窗口右击服务器名称（例如 ATEN-01），在弹出的快捷菜单中选择【使服务器成为一级服务器】命令，如图 2-28 所示。

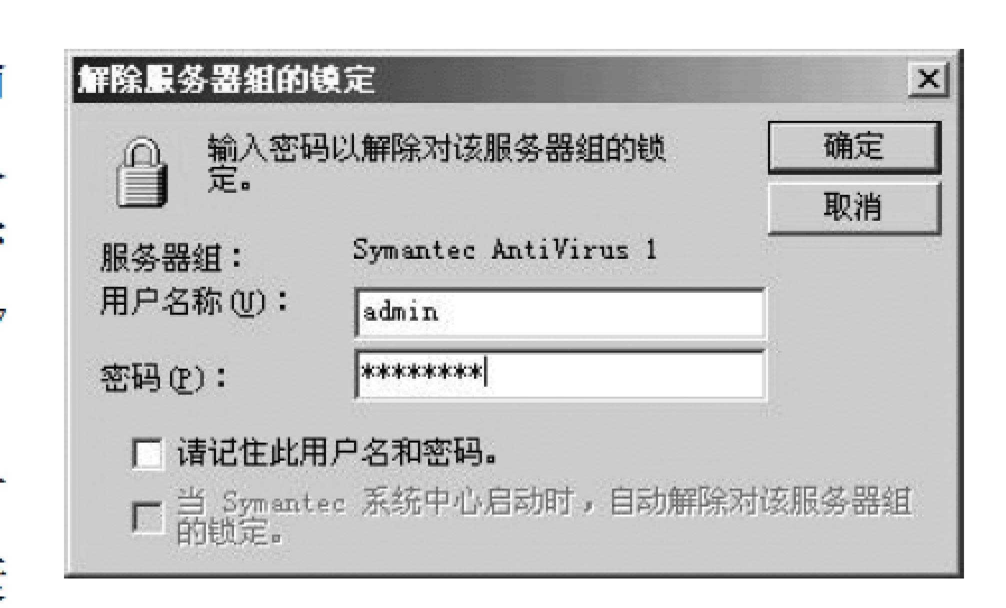


图 2-27　输入用户名和密码

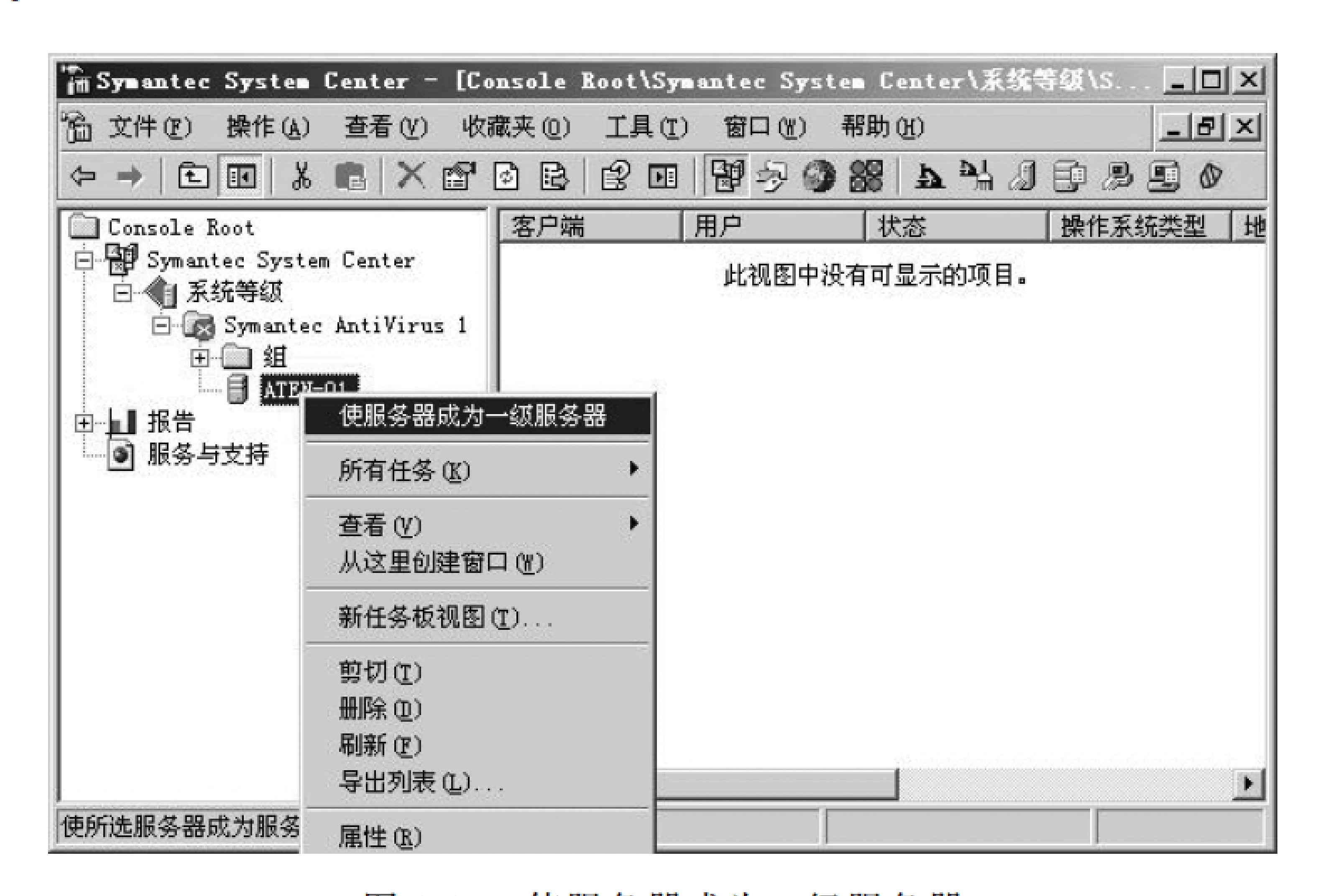


图 2-28　使服务器成为一级服务器

（17）在【是否要继续】对话框中单击【是】按钮，如图 2-29 所示。

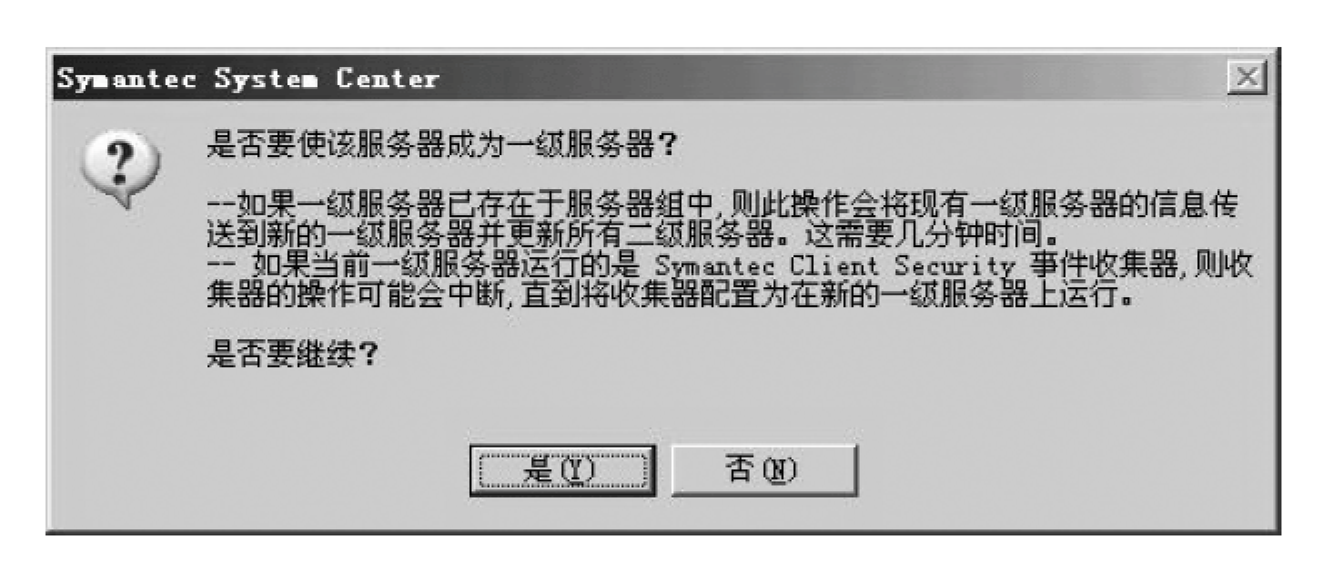


图 2-29　确认是否要使服务器成为一级服务器

3. 安装 LiveUpdate 管理实用工具

（1）在 Symantec 主菜单上选择【安装其他管理员工具】命令，如图 2-30 所示。

（2）在【安装其他管理员工具】菜单上选择【安装 LiveUpdate Administrator】命令，如图 2-31所示。

（3）在【选择目标位置】对话框中，选择程序安装目标文件夹，如图 2-32 所示。

（4）在【安装完毕】对话框中，单击【完成】按钮，如图 2-33 所示。





图 2-30　Symantec 主菜单

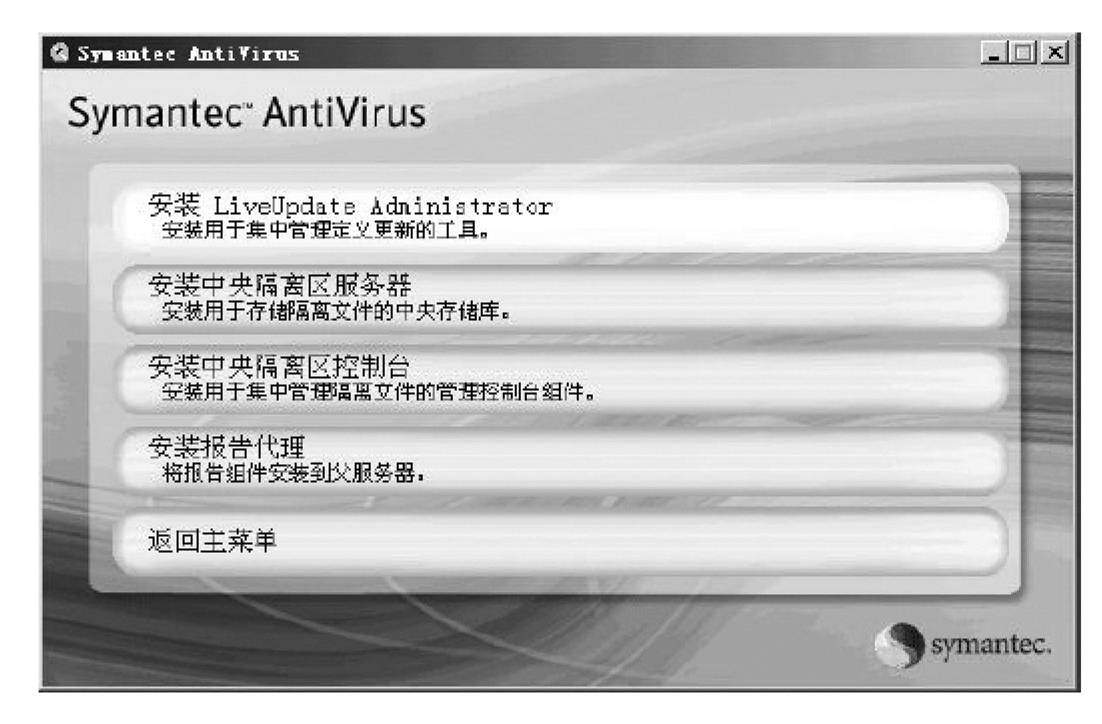


图 2-31　选择【安装 LiveUpdate Administrator】命令

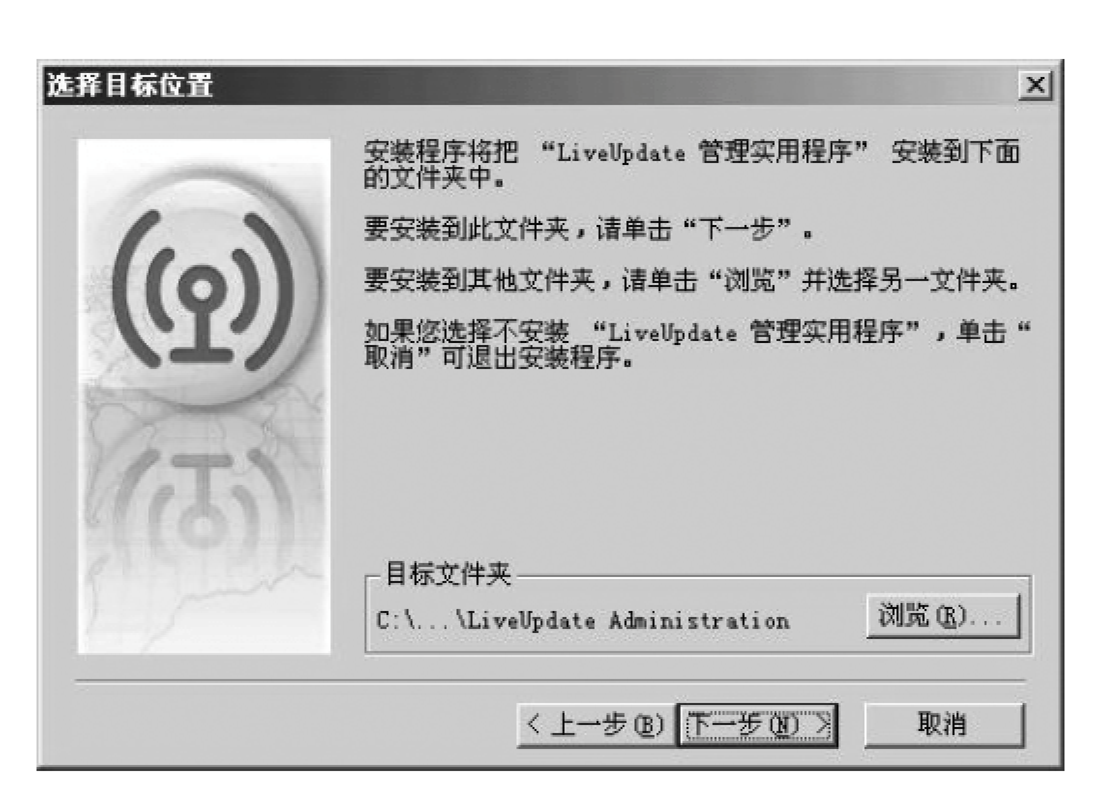


图 2-32　选择安装目标位置



图 2-33　安装完毕

4. 安装中央隔离区服务器

(1) 在【安装其他管理员工具】菜单上选择【安装中央隔离区服务器】命令，如图 2-34 所示。



图 2-34　选择【安装中央隔离区服务器】命令

(2) 在【授权许可协议】对话框中，选择【我接受该许可证协议中的条款】单选按钮，单击【下一步】按钮，如图 2-35 所示。

(3) 在【目标文件夹】对话框中，单击【更改】按钮，可以更改程序安装的位置，单击【下一步】按钮，如图 2-36 所示。



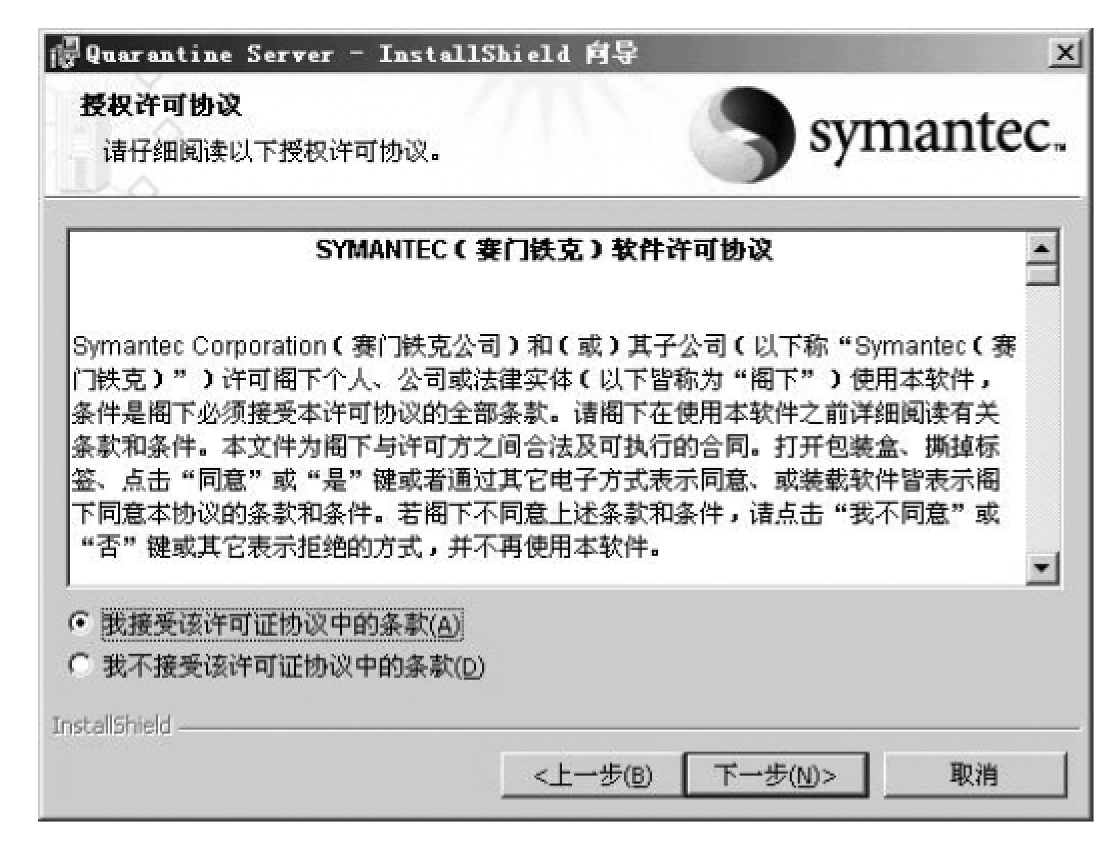


图 2-35　授权许可协议



图 2-36　选择安装目标文件夹

（4）在【安装类型】对话框中，选择【基于 Internet（推荐）】单选按钮，单击【下一步】按钮，如图 2-37所示。

（5）在【最大磁盘空间】对话框中输入提供给隔离区的最大磁盘空间（例如 400），单击【下一步】按钮，如图 2-38 所示。

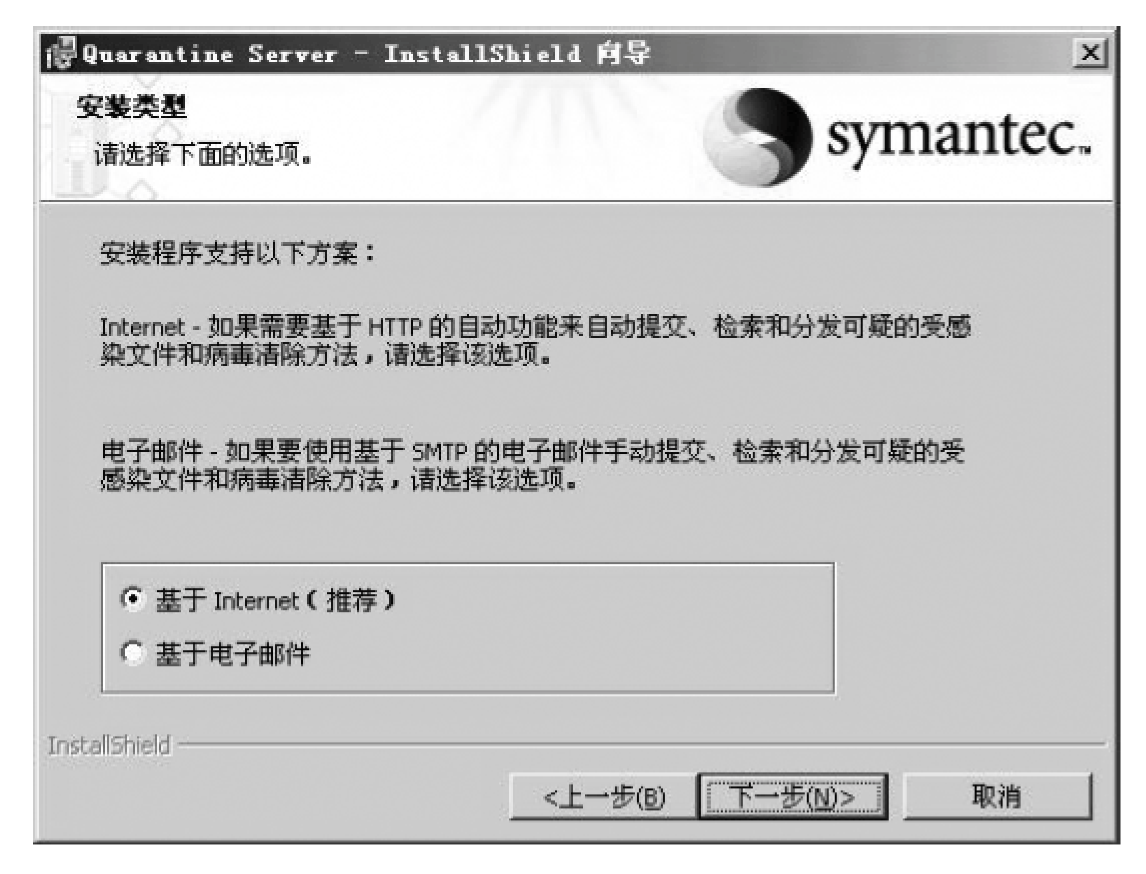


图 2-37　选择安装类型



图 2-38　输入最大磁盘空间

（6）在【联系信息】对话框中输入相关信息，单击【下一步】按钮，如图 2-39 所示。

（7）在【Web 通信】对话框中输入网关名称，可以选择默认值，然后单击【下一步】按钮，如图 2-40 所示。

（8）在【警报配置】对话框中，选中【启用警报】复选框，在服务器名称的文本框中输入服务器名称（例如 ATEN-01），单击【下一步】按钮，如图 2-41 所示。

（9）在【InstallShield 向导完成】对话框单击【完成】按钮，如图 2-42 所示。

5. 安装中央隔离区控制台

在【安装其他管理员工具】菜单中选择【安装中央隔离区控制台】命令，如图 2-43 所示。整个部署过程比较简单，按照向导提示，选择默认值即可。







图 2-39　输入联系信息



图 2-40　输入网关名称



图 2-41　警报配置



图 2-42　安装完成



图 2-43　选择【安装中央隔离区控制台】命令

6．部署 Symantec 客户端程序

利用"客户端远程安装"工具就可以在知道 Windows 2000/XP/Server 2003 系统管理员密码的基础上给这些系统远程安装 NAV 10.1 的受管理的防病毒客户端，以及受管理的防病毒客户端的病毒码升级，管理策略可以由服务器统一管理。客户端的安装还可以用



Web 安装、从防病毒服务器共享目录安装、安装时选择【受管理的】安装方式等多种安装方法。在此，以利用“客户端远程安装”工具为例，介绍 Symantec 客户端程序的安装。

（1）在【Symantec 系统中心控制台】窗口，选择【工具】/【客户端远程安装】命令，如图 2-44所示。

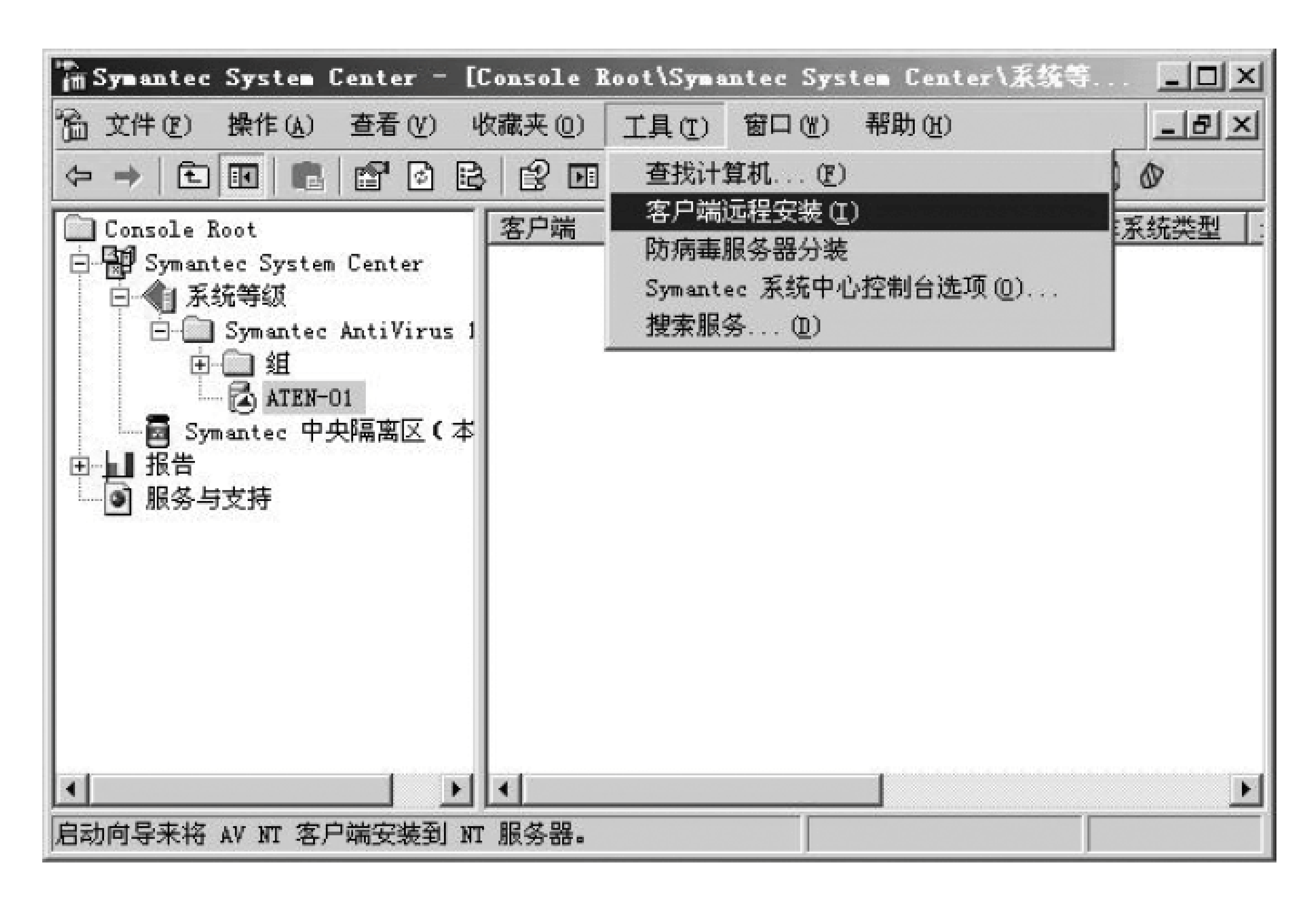


图 2-44　选择【客户端远程安装】命令

（2）在【选择安装来源的位置】对话框中选择【默认位置】单选按钮，单击【下一步】按钮，如图 2-45 所示。

（3）在【选择计算机】对话框的右边选择服务器（例如 ATEN-01），在左边选择可用的客户机（例如 Pro_a、Xp-a 等），单击【添加】按钮，将客户机添加到右边的列表框，然后单击【完成】按钮，如图 2-46 所示。




图 2-45　选择安装来源的位置

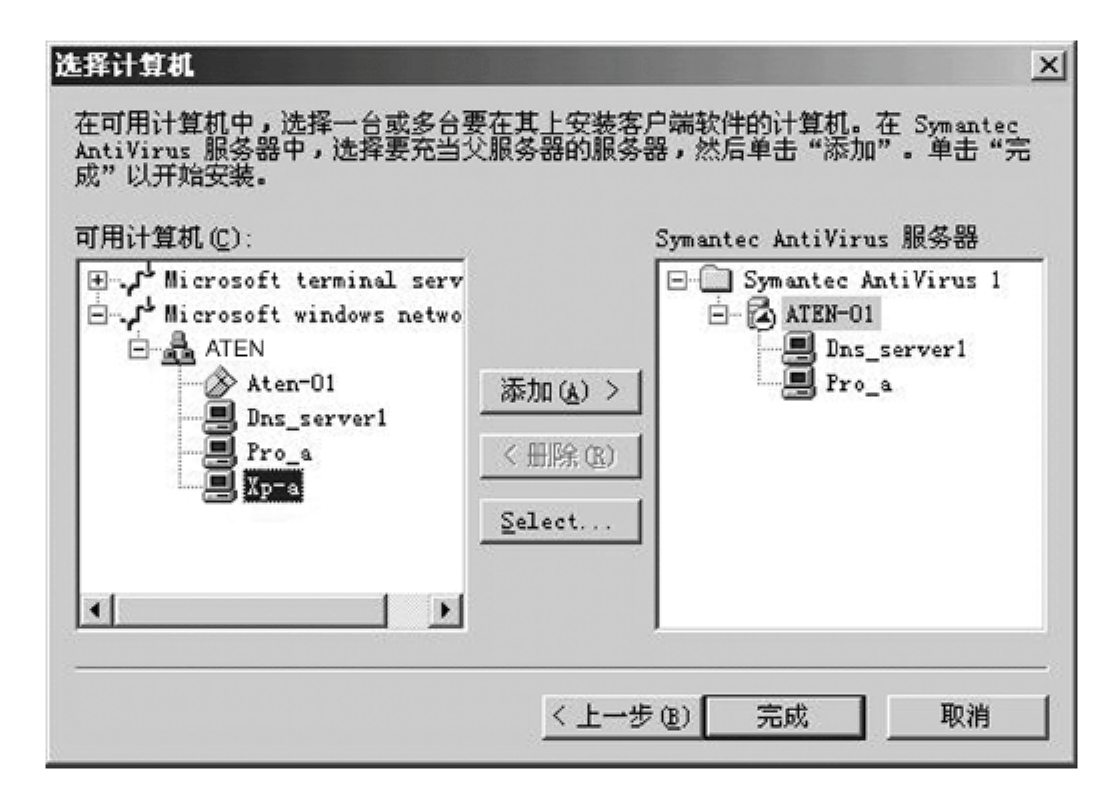


图 2-46　选择计算机

（4）在【远程客户端安装的状态】对话框中，单击【完成】按钮，如图 2-47 所示。

2.3.3　设置 Symantec 控制台

Symantec 服务器的主要管理功能有如下几个方面。

（1）系统补丁的安装。Symantec 服务器与客户机通过微软的官方网站下载补丁，在企





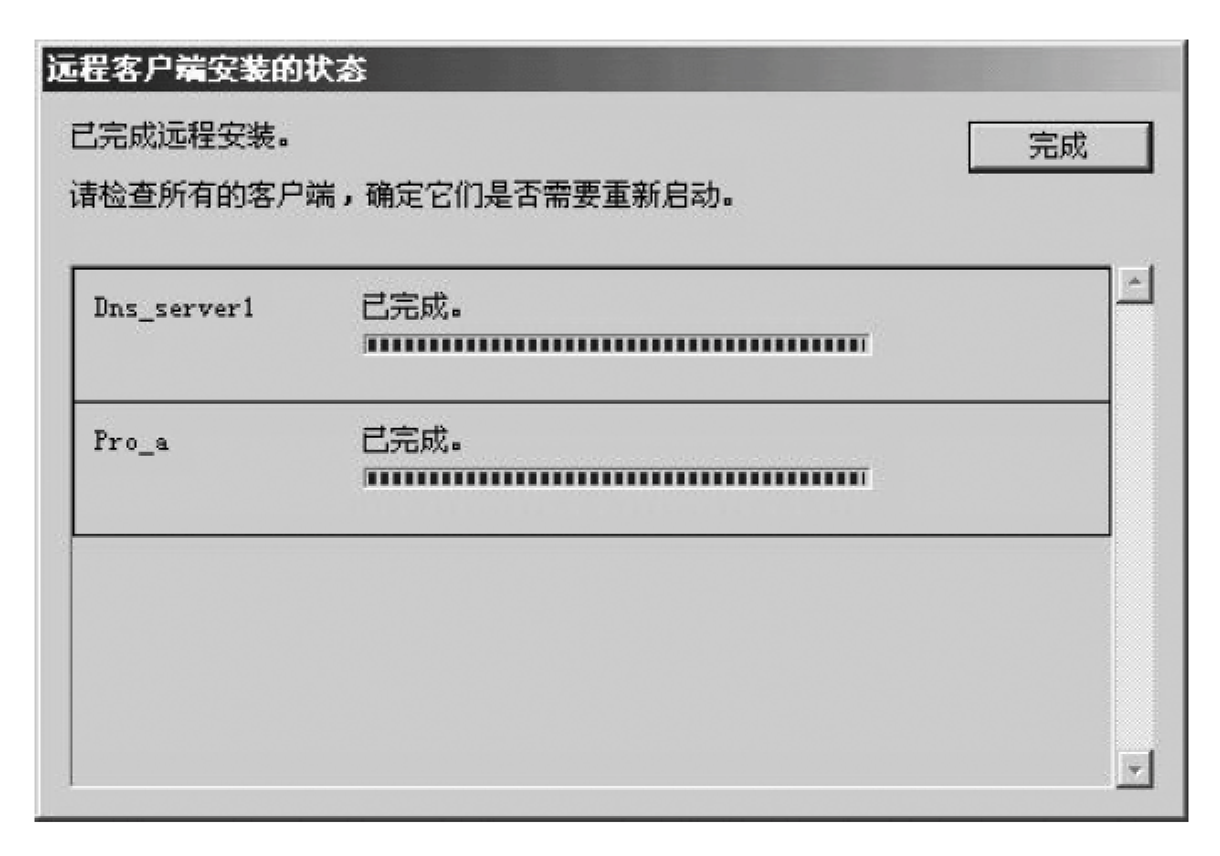


图 2-47　远程客户端安装的状态

业内部可以通过 SUS(Windows Server Update Service，Windows 更新服务)实现补丁的自动安装。

(2) 部署防病毒策略。设定发现病毒时的处理办法，防止客户端删除防病毒程序，定期自动扫描客户端，防止客户端关闭实时防护等。

(3) 病毒码更新。自动更新或手动更新，客户端的病毒码会随着 Symantec 服务器的病毒码的升级而自动升级。

1. 部署 LiveUpdate 更新

(1) 在【Symantec 系统中心控制台】窗口，右击 Symantec 服务器(ATEN-01)，在弹出的菜单中选择【所有任务】/【LiveUpdate】/【配置】命令，如图 2-48 所示。



图 2-48　配置 LiveUpdate

(2) 在 LiveUpdate 选项卡中，可以配置 LiveUpdate 源的参数，建议选择默认值，如图 2-49所示。



（3）在【LiveUpdate 管理员】选项卡中，可以配置 LiveUpdate 包检索的频率和时间，然后单击【确定】按钮，如图 2-50 所示。

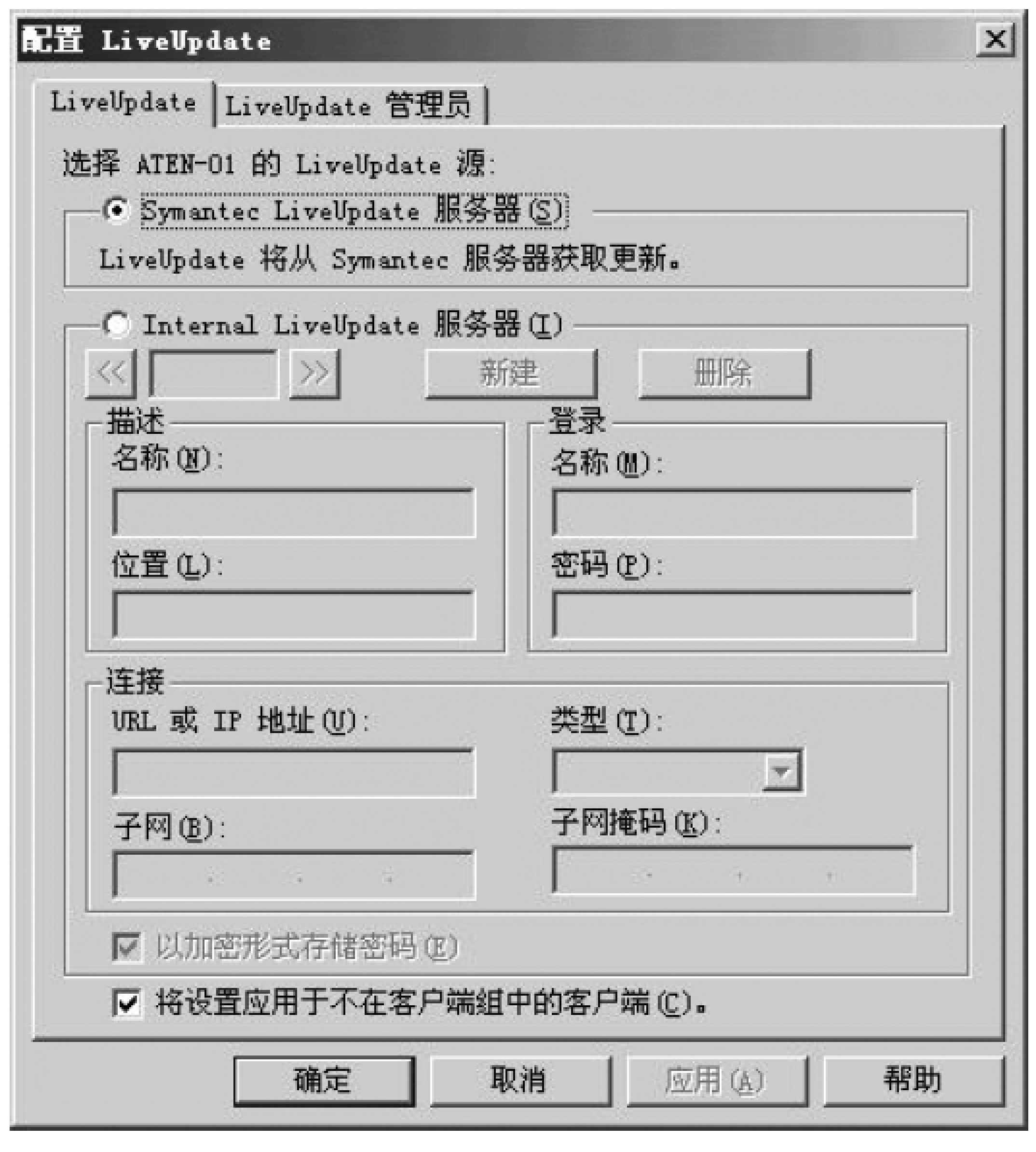


图 2-49　LiveUpdate 选项卡



图 2-50　【LiveUpdate 管理员】选项卡

2. 定义病毒库更新策略

（1）在【Symantec 系统中心控制台】窗口，右击 Symantec 服务器（ATEN-01），在弹出的菜单中选择【所有任务】/【Symantec AntiVirus】/【病毒定义管理器】命令，如图 2-51 所示。

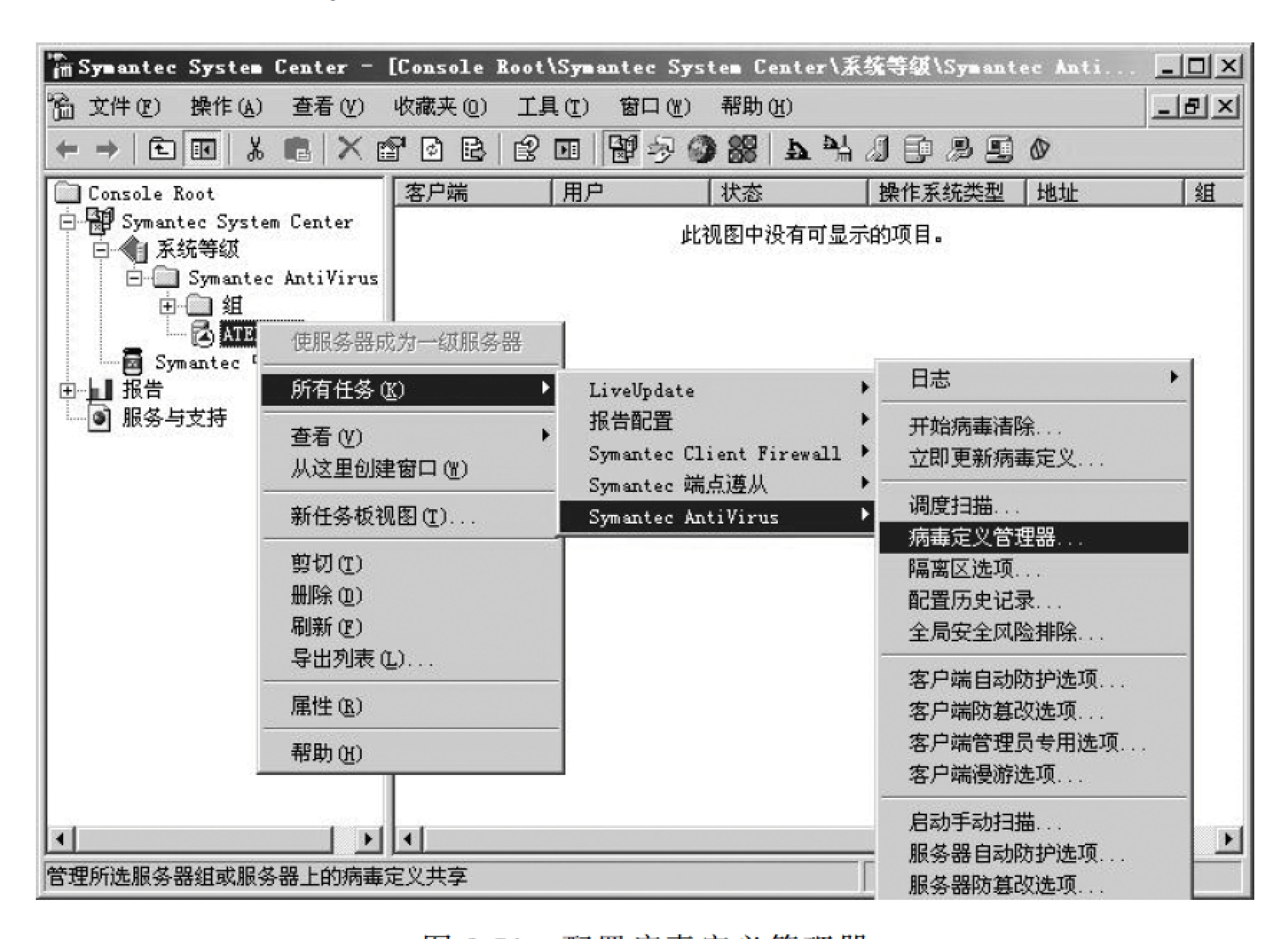


图 2-51　配置病毒定义管理器





（2）在【病毒定义管理器】对话框中，单击【只更新此服务器组中的一级服务器】右侧的【配置】按钮，在打开的【设置一级服务器更新】对话框中选中【调度自动更新】复选框，单击【调度】按钮，配置调度参数（如更新的频率和时间等），然后单击【确定】按钮，如图 2-52 所示。

（3）在【病毒定义管理器】对话框中，选中【从父服务器更新病毒定义】复选框，然后单击此项右边的【设置】按钮；在打开的【更新设置】对话框中设置检查更新的时间间隔（例如 60 分钟），然后两次单击【确定】按钮，如图 2-53 所示。

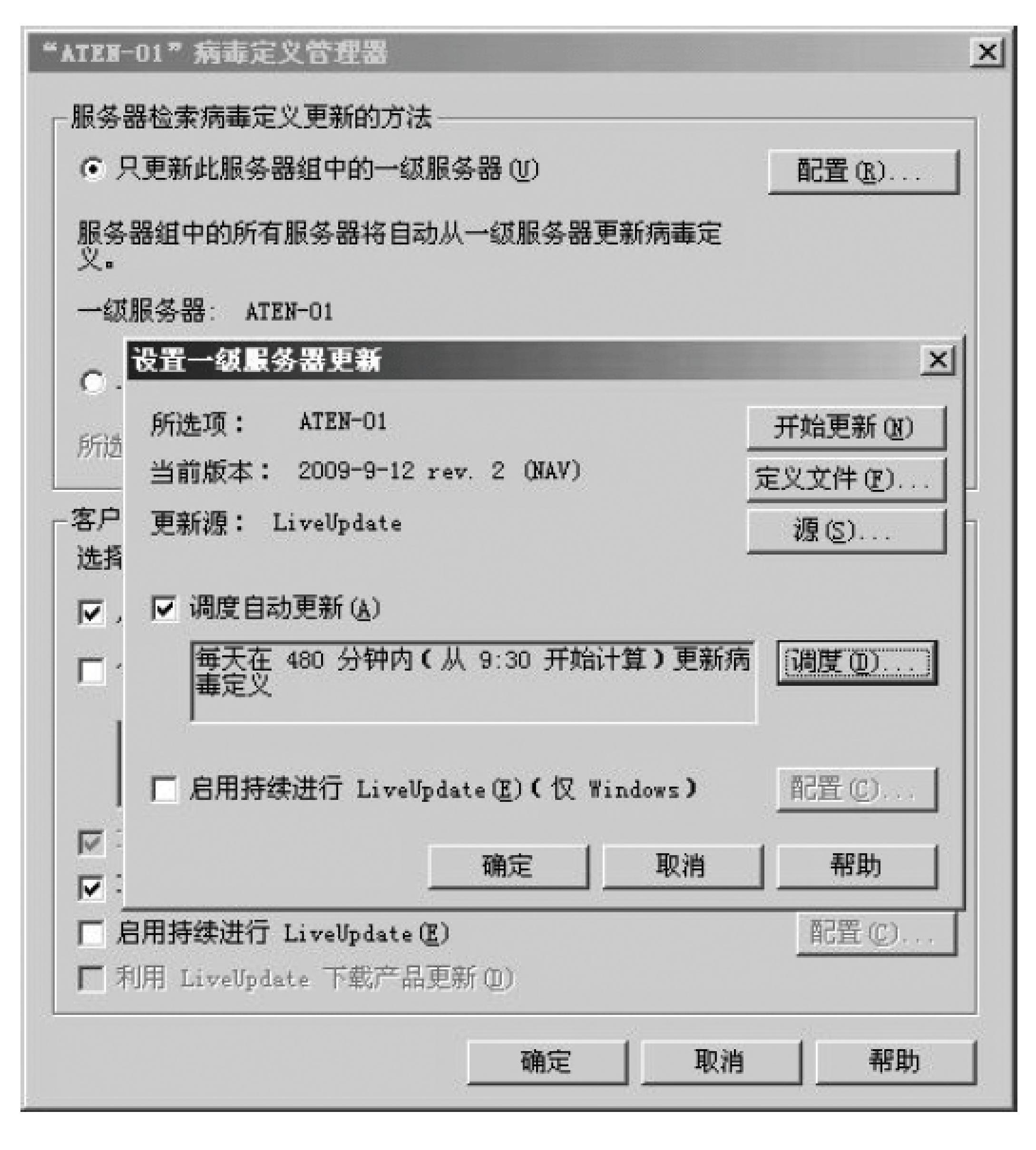


图 2-52　设置一级服务器的更新时间



图 2-53　设置客户端的更新时间

3. 设置服务器和客户端定时扫描的策略

（1）在【Symantec 系统中心控制台】窗口，右击 Symantec 服务器（ATEN-01），在弹出的菜单中选择【所有任务】/Symantec AntiVirus/【调度扫描】命令，如图 2-54 所示。

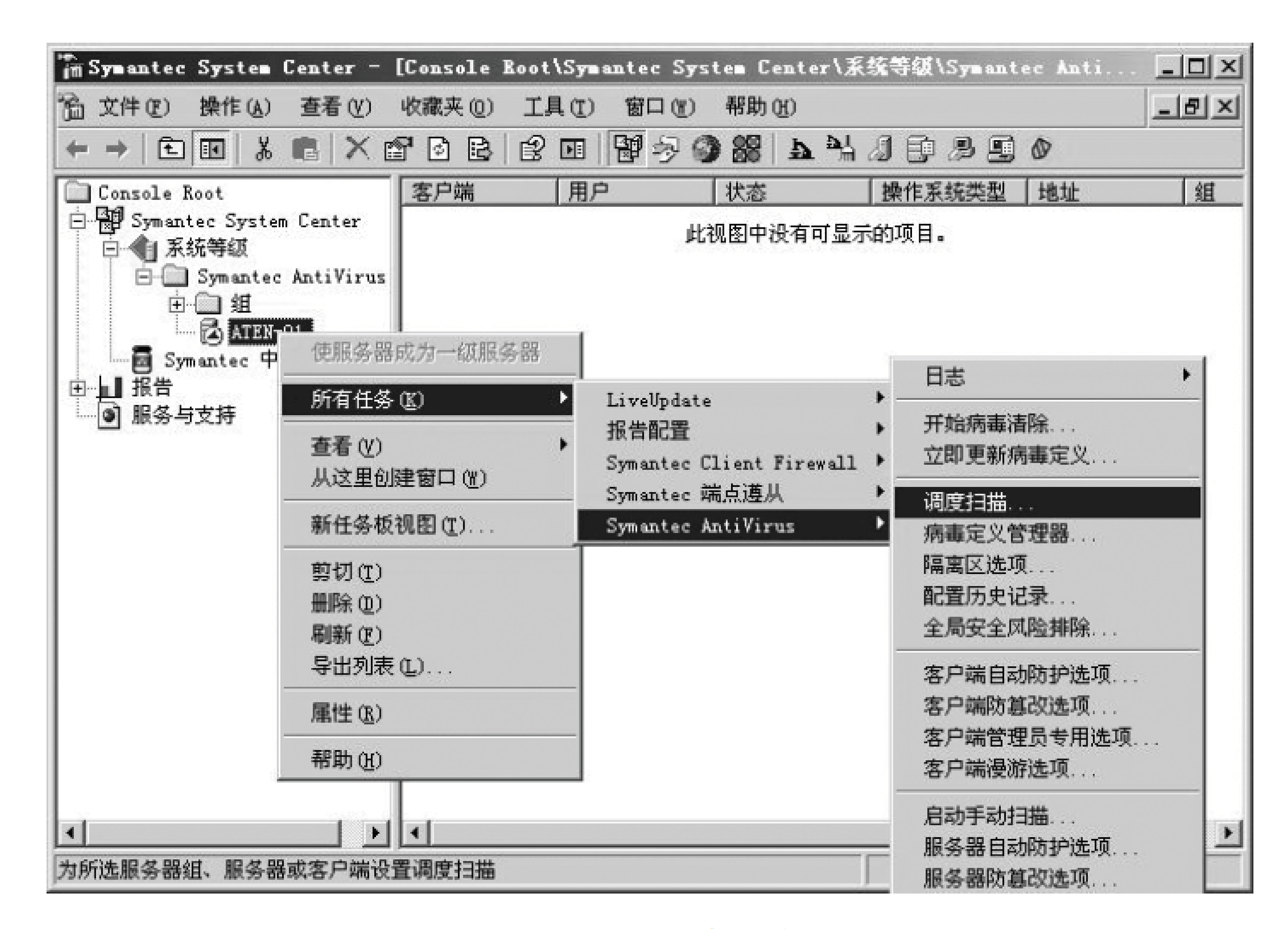


图 2-54　调度病毒扫描



(2) 在【调度扫描】对话框中打开【服务器扫描】选项卡,单击【新建】按钮,在【ATEN-01 调度扫描】对话框中设置服务器扫描参数,单击【确定】按钮,如图 2-55 所示。

(3) 打开【客户端扫描】选项卡,按上述方法创建客户端扫描调度,最后单击【确定】按钮,如图 2-56 所示。

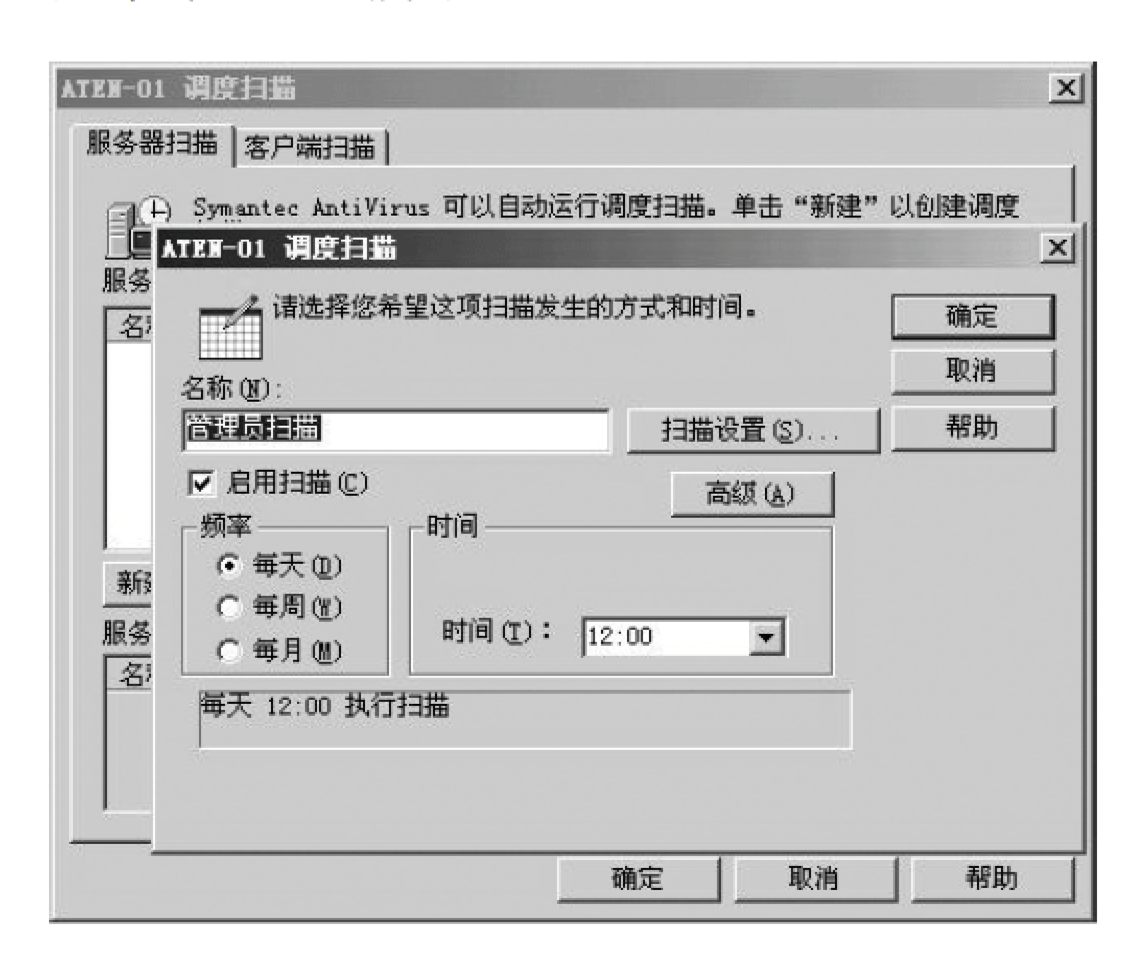




图 2-55　创建服务器扫描

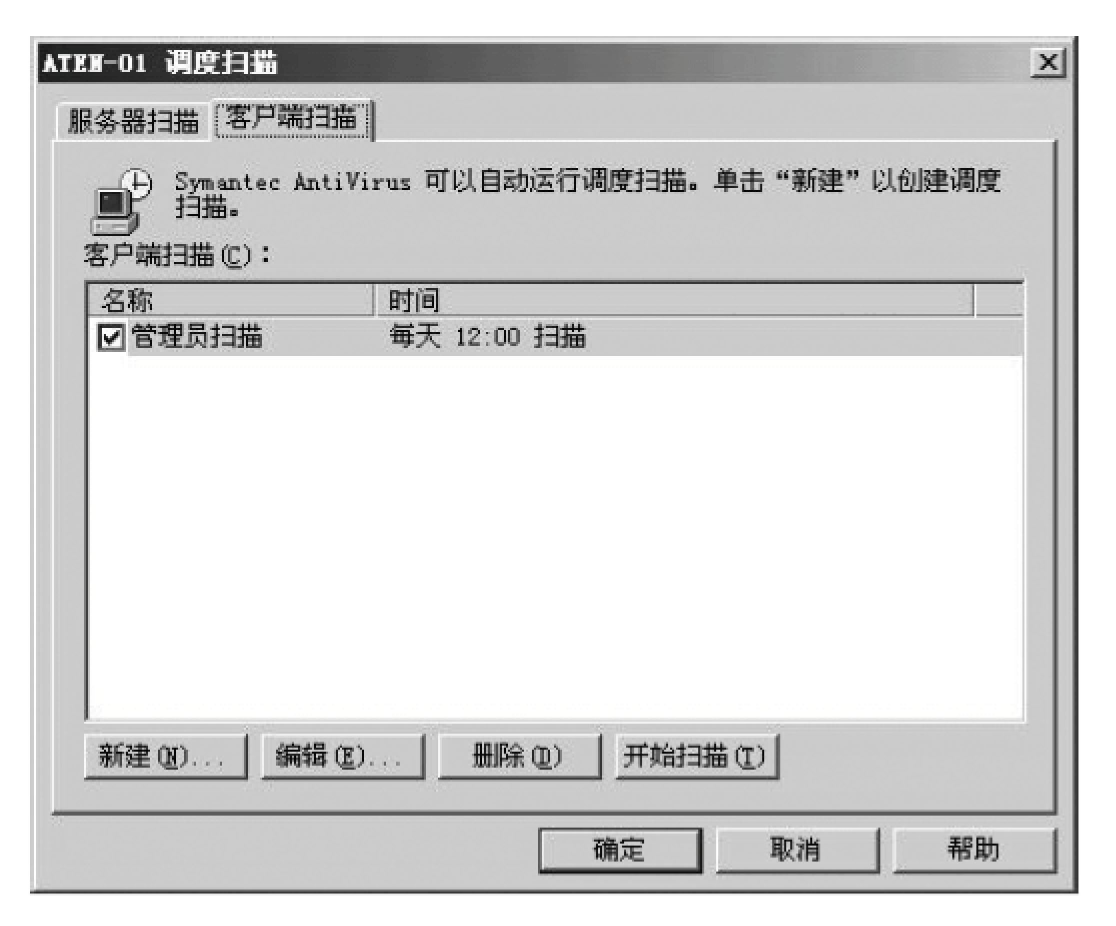


图 2-56　创建客户端扫描

4. 设置隔离区选项

(1) 在【Symantec 系统中心控制台】窗口,右击 Symantec 服务器(ATEN-01),在弹出的菜单中选择【所有任务】/Symantec AntiVirus/【隔离区选项】命令,如图 2-57 所示。

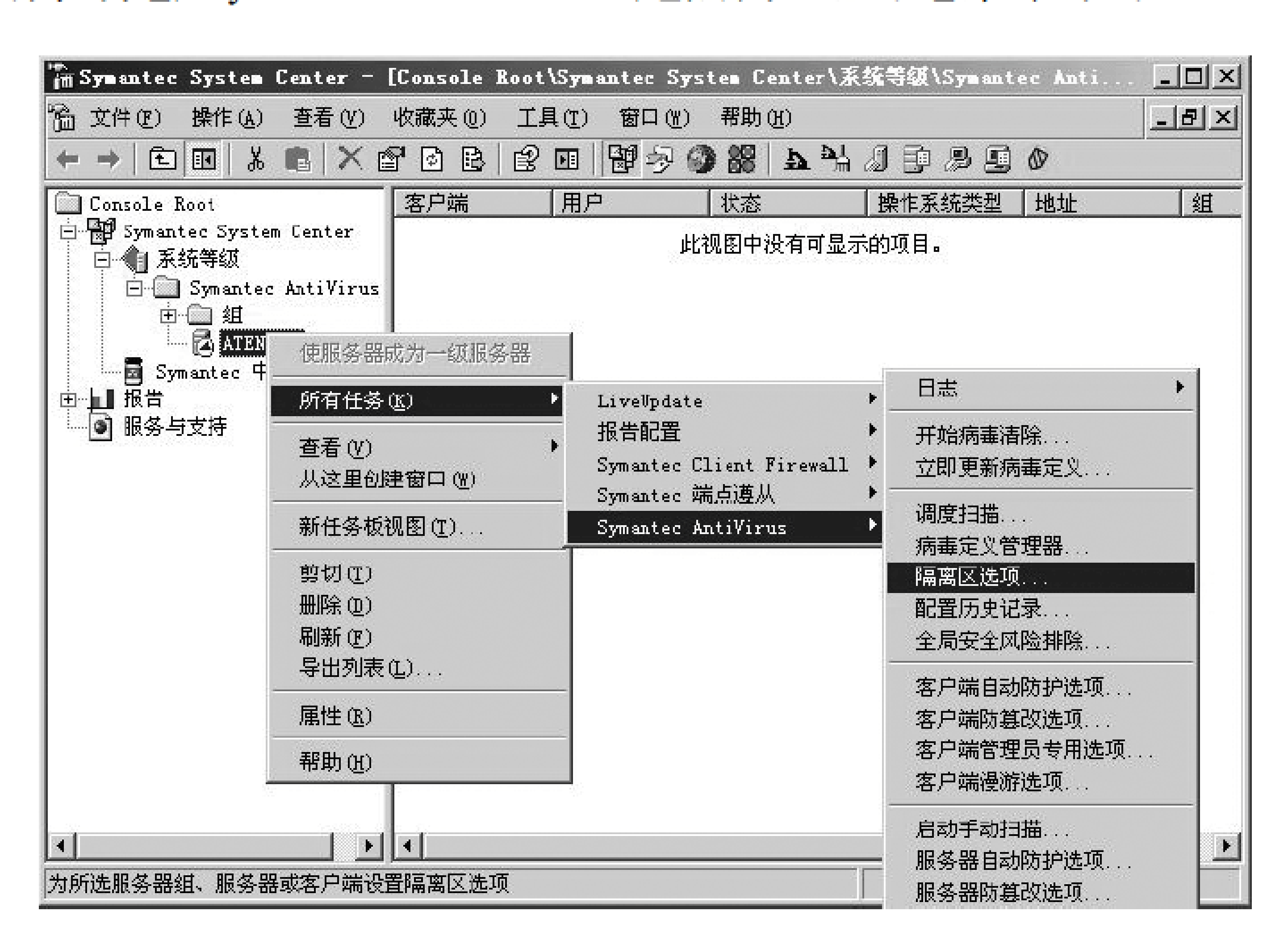


图 2-57　隔离区选项

(2) 在【隔离区选项】对话框中配置端口、重试、协议等相关参数,然后单击【确定】按钮,如图 2-58 所示。

(3) 在【Symantec 系统中心控制台】窗口,右击【Symantec 中央隔离区】,在弹出的菜单中选择【附加到服务器】命令,如图 2-59 所示。





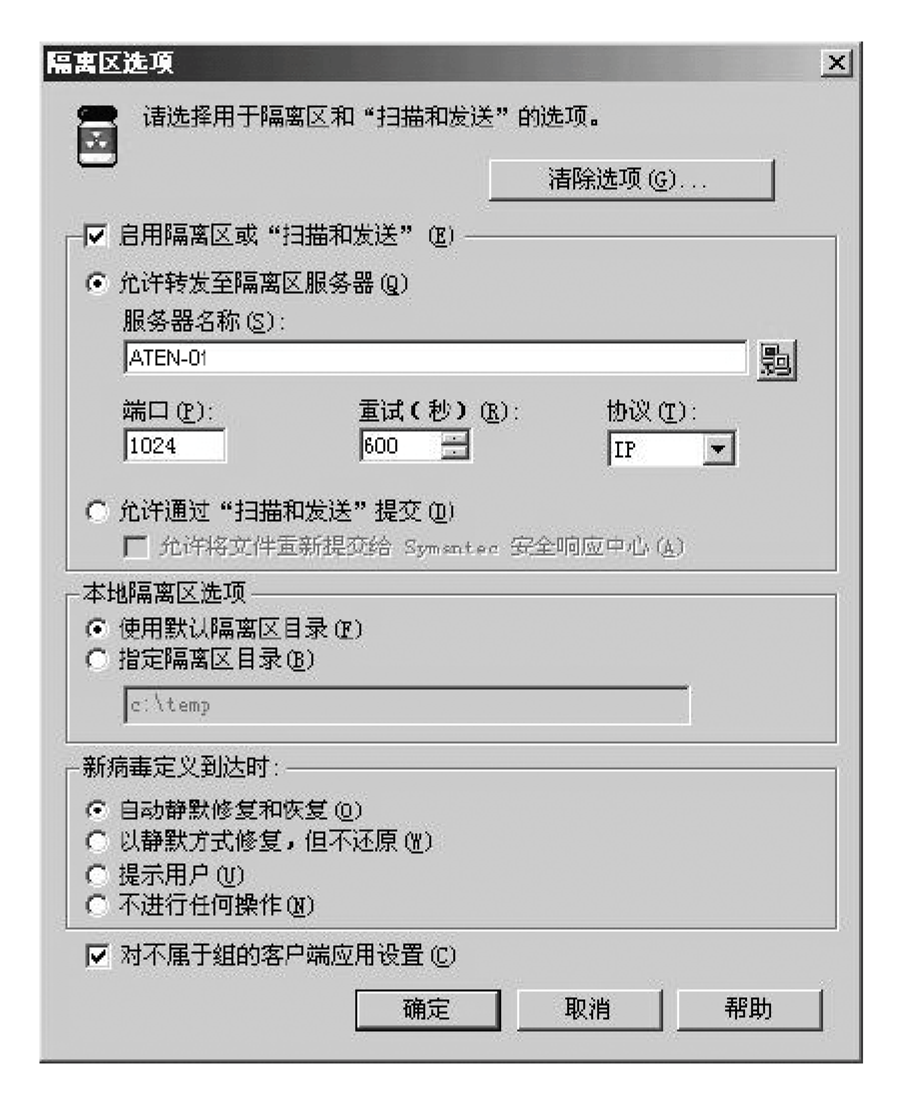


图 2-58　【隔离区选项】对话框



图 2-59　Symantec 中央隔离区附加到服务器

(4) 在【选择计算机】对话框中选择【本计算机】单选按钮，单击【完成】按钮，如图 2-60 所示。

(5) 在【附加到隔离区服务器】对话框中输入服务器的名称，单击【确定】按钮，如图 2-61 所示。

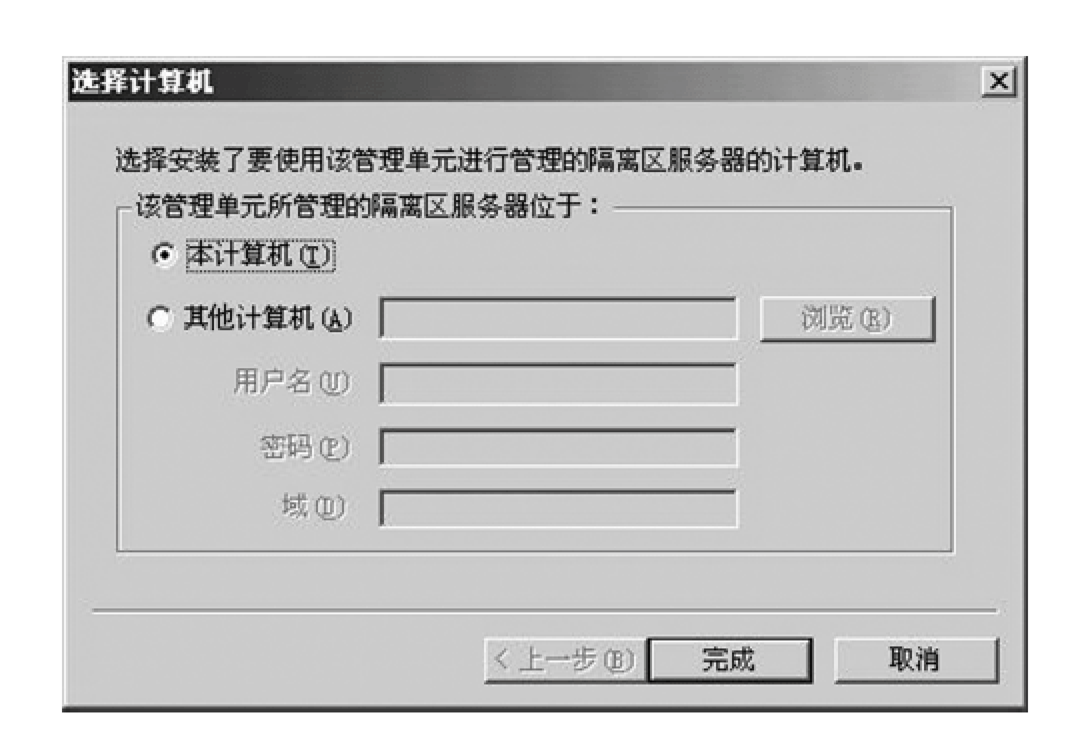


图 2-60　选择【本计算机】



图 2-61　输入服务器名称

2.3.4　Symantec 网络防病毒系统应用

Symantec 网络防病毒系统部署完成后，可以在 Symantec 服务器(例如 ATEN-01)对整个网络进行病毒库更新、查毒和杀毒。

如图 2-62 所示，在客户端列表中，右击选中的客户机(可以选择一台或多台)，在弹出的菜单中选择【所有任务】/Symantec AntiVirus/【立即更新病毒定义】命令，可以更新客户端的病毒库，或者手动查毒和杀毒。





图 2-62　对客户端的查毒和杀毒

2.4　蠕虫病毒

蠕虫病毒是一种常见的计算机病毒。它的传染机理是利用网络进行复制和传播，传染途径是通过网络、电子邮件以及 U 盘、移动硬盘等移动存储设备。比如 2003 年肆虐的“冲击波”和 2004 年的“震荡波”、“狙击波”，2006 年以来危害极大的“维金”（Worm. Viking. m，也称“威金”）、“熊猫烧香”（Worm. WhBoy. h，也称“武汉男孩”）都是蠕虫病毒的一种。蠕虫程序主要利用系统漏洞进行传播。它通过网络、电子邮件和其他传播方式，像生物蠕虫一样从一台计算机传染到另一台计算机。因为蠕虫使用多种方式进行传播，所以蠕虫程序的传播速度是非常快的。

蠕虫侵入一台计算机后，首先获取其他计算机的 IP 地址，然后将自身副本发送给这些计算机。蠕虫病毒也使用存储在染毒计算机上的邮件客户端地址簿里的地址来传播程序。虽然有的蠕虫程序也在被感染的计算机中生成文件，但一般情况下，蠕虫程序只占用内存资源而不占用其他资源。

蠕虫通常会感染目前主流的 Windows 2000/XP/Server 2003 系统，如果不及时预防，它们会蚕食并破坏系统，最终使整个系统瘫痪，并有可能会在几天内快速传播，大规模感染网络，对网络安全造成严重危害。

2.4.1　蠕虫病毒的定义和危害性

1. 蠕虫的定义

蠕虫本来只是一个生物学名词，在 1982 年由 Shock 和 Hupp 引入计算机领域，并给出了计算机蠕虫的两个最基本特征，即可以从一台计算机移动到另一台计算机，并且可以自我复制。1988 年 Morris 蠕虫爆发后，为了区分蠕虫和病毒，从技术的角度给出了蠕虫的定义：“计算机蠕虫可以独立运行，并能把自身的一个包含所有功能的版本传播到另外的计算机上”。

2. 蠕虫与一般病毒的区别

由于蠕虫和病毒具有共同特征，人们常常将蠕虫当作病毒。

一般的病毒是需要寄生的，它可以通过自己指令的执行，将自己的指令代码写到其他程序的体内，而被感染的文件就被称为“宿主”。例如，在 Windows 下可执行文件的格式为 pe(Portable Executable，可移植可执行)格式，当需要感染 pe 文件时，在宿主程序中建立一个新节，将病毒代码写到新节中，或修改程序入口点等。这样，宿主程序执行的时候，就可以先执行病毒程序，病毒程序运行完之后，再把控制权交给宿主原来的程序指令。可见，病毒主要是感染文件。

但蠕虫一般不采取利用 pe 格式插入文件的方法，而是复制自身在 Internet 环境下进行传播，病毒的传染能力主要是针对计算机内的文件系统而言。蠕虫的传染目标是 Internet 内的所有计算机或局域网条件下的共享文件夹、电子邮件、网络中的恶意网页，以及大量存在着漏洞的服务器等都成为蠕虫传播的良好途径。

由于蠕虫和计算机病毒都具有传染性与复制功能，导致两者之间是非常难区分的。尤其是近年来，越来越多的病毒采取了部分蠕虫的技术。另外，具有破坏性的蠕虫也采取了部分病毒的技术，于是后来就把两类程序统称为“蠕虫病毒”。

蠕虫病毒通过不停地获得网络中存在漏洞的计算机上的部分或全部控制权来进行传播，它的最大特点就是大量侵占系统或网络带宽资源，造成用户计算机和网络通信效率大大降低，甚至瘫痪。蠕虫病毒与计算机病毒的主要区别如表 2-2 所示。

表 2-2　蠕虫病毒与计算机病毒的比较

比较项目	蠕虫病毒	计算机病毒(传统)
存在形式	独立个体	寄生
复制机制	自身的复制	插入到宿主文件
传染机制	系统漏洞	宿主程序运行(需要运行病毒文件或含病毒文件)
攻击目标	网络上的其他计算机	本地文件
触发机制	程序自身	计算机使用者
影响重点	网络性能和系统性能	文件系统
计算机使用者的角色	无关	传播中的关键环节
防治措施	为系统打补丁	从宿主文件中清除
对抗主体	系统软件、服务软件提供商和网络管理人员	计算机使用者和反病毒的厂商

3. 蠕虫病毒的危害

根据使用者情况，可将蠕虫病毒分为两种。一种是对企业用户和局域网而言，这种蠕虫病毒利用系统漏洞，主动进行攻击，可以对整个 Internet，可造成瘫痪性的后果，以红色代码、尼姆达蠕虫，以及 SQL 蠕虫王为代表。另外一种是针对个人用户的，它通过网络(主要是电子邮件、恶意网页形式)迅速传播蠕虫，以爱虫蠕虫、求职信蠕虫为代表。在这两种蠕虫中，第一种具有很大的主动攻击性，而且爆发有一定的突然性，但相对来说，查杀这种蠕虫并



不是很难。第二种蠕虫的传播方式比较复杂和多样，少数利用了微软的应用程序的漏洞，更多的是利用社会工程学对用户进行欺骗和诱使。这样的蠕虫造成的损失非常大，同时也很难根除。比如求职信蠕虫，在 2001 年就已经被各大杀毒厂商发现，但直到 2002 年年底依然排在病毒危害排行榜的首位。

蠕虫病毒是目前危害最大的恶意程序，几乎每次蠕虫发作都会造成巨大的经济损失。1988 年 11 月 2 日，Morris 蠕虫发作，几天之内 6000 台以上的 Internet 服务器因感染而瘫痪，损失超过 1000 万美元；2001 年 7 月 19 日，CodeRed 蠕虫爆发，爆发后的 9 个小时内就攻击了 25 万台计算机，造成的损失估计超过 20 亿美元，随后几个月内产生了威力更强的几个变种，其中 CodeRed Ⅱ造成的损失估计超过 12 亿美元；2001 年 9 月 18 日，Nimda 蠕虫被发现，对 Nimda 造成的损失的评估数据从 5 亿美元攀升到 26 亿美元后，继续攀升，到现在已无法估计。直到现在仍在全球爆发的"冲击波"蠕虫病毒及其变种，其传播速度及危害之大是史无前例的。与以前的蠕虫病毒相比，"冲击波"的感染潜力大得多，由于在全球范围内微软操作系统的漏洞影响的计算机数量庞大，因此，其危害很难在近期内统计出来。目前蠕虫病毒爆发的频率越来越高，尤其是近两年来，越来越多的蠕虫病毒出现，其传播速度以几何级数增长，危害之大始料不及。

2.4.2　蠕虫病毒的工作模式

蠕虫病毒由两部分组成：一个主程序和一个引导程序。主程序一旦在机器上建立，就会去收集与当前机器联网的其他机器的信息。它能通过读取公共配置文件并运行显示当前网上联机状态信息的系统实用程序而做到这一点。随后，它尝试利用系统的缺陷在这些远程机器上建立其引导程序。

蠕虫病毒程序常驻于一台或多台机器中，并有自动重新定位(AutoRelocation)的能力。如果它检测到网络中的某台机器未被占用，它就把自身的一个副本(一个程序段)发送给那台机器。每个程序段都能把自身的副本重新定位于另一台机器中，并且能识别它占用的那台机器。

2.4.3　蠕虫病毒的基本特征

通过对蠕虫的整个工作流程进行分析，可以归纳出它的行为特征如下。

1. 主动攻击

蠕虫在本质上已经演变为黑客入侵的自动化工具。当蠕虫被释放后，从搜索漏洞，到利用搜索结果攻击系统，到复制副本，整个流程全由蠕虫自身主动完成。

2. 行踪隐蔽

由于蠕虫的传播过程不像病毒那样需要计算机使用者的辅助工作(如执行文件、打开文件、阅读信件、浏览网页等)，所以在蠕虫传播的过程中计算机使用者基本上不可察觉。

3. 利用系统、网络应用服务漏洞

除了最早的蠕虫在计算机之间传播，是程序设计人员许可并在每台计算机上做了相应



的配合支持机制之外，所有后来的蠕虫都要突破计算机系统的自身防线，并对其资源进行滥用。计算机系统存在漏洞是蠕虫传播的前提，利用这些漏洞，蠕虫获得被攻击的计算机系统的相应权限，完成后面的复制和传播过程。这些漏洞有的是操作系统本身的问题，有的是应用服务程序的问题，有的是网络管理人员的配置问题。正是由于漏洞产生原因的复杂性，导致面对蠕虫的攻击防不胜防。

4. 造成网络拥塞

蠕虫进行传播的第一步就是找到网络上其他存在漏洞的计算机系统，这需要通过大面积的搜索来完成。搜索动作包括：判断其他计算机是否存在，判断特定应用服务是否存在，判断漏洞是否存在。这不可避免地会产生附加的网络数据流量。即使是不包含破坏系统正常工作的恶意代码的蠕虫，也会因为它产生了巨大的网络流量而导致整个网络瘫痪，从而造成经济损失。

5. 降低系统性能

蠕虫入侵到计算机系统之后，会在被感染的计算机上产生自己的多个副本，每个副本启动搜索程序寻找新的攻击目标。大量的进程会耗费系统的资源，导致系统的性能下降。这对网络服务器的影响尤其明显。

6. 产生安全隐患

大部分蠕虫会收集、扩散、暴露系统敏感信息(如用户信息等)，并在系统中留下后门，有些还与黑客技术相结合。这些都会导致未来的安全隐患。以红色代码为例，感染后的机器的 Web 目录的\scripts 下将生成一个 Root.exe，可以远程执行任何命令，从而使黑客能够再次进入。

7. 反复性

即使清除了蠕虫在文件系统中留下的任何痕迹，如果没有修补计算机系统漏洞，重新接入到网络中的计算机还是会被重新感染。这个特性在 Nimda 蠕虫的身上表现得尤为突出。计算机使用者用一些声称可以清除 Nimda 的防病毒产品来清除本机上的 Nimda 蠕虫副本后，很快又重新被 Nimda 蠕虫所感染。

8. 编写过程简单

蠕虫病毒的编写过程简单，不需要经过复杂的学习。它们往往就是利用 VBS 来编写的。比如欢乐时光这类病毒，只要仔细研究它们的源代码，很快就可以自己编写一个相似的病毒出来。这样，利用 VBS 或者相似技术编写的病毒越来越多。同时，由于其简单性，甚至可以编写出专门生产病毒的程序。尽管这一类程序在技术上可能没有太多创新，但在当前的反病毒技术下，防病毒软件并不可以识别这些具有相似性的病毒。

蠕虫病毒制作技术与传统的病毒不同的是，许多新病毒是利用当前最新的编程语言与编程技术实现的，易于修改，以产生新的变种，从而逃避反病毒软件的搜索。另外，新病毒利用 Java、ActiveX、VBScript 等技术，可以潜伏在 HTML 页面里，在上网浏览时触发。



9. 传播方式多样

如 Nimda 病毒和求职信病毒就有多种传播方式，可利用的传播途径包括文件、电子邮件、Web 服务器、网络共享等。

2.4.4 蠕虫病毒的预防措施

蠕虫病毒和普通病毒一个不同的特征是蠕虫病毒往往能够利用漏洞。这里的漏洞或者说是缺陷，可分为两种：软件上的缺陷和人为的缺陷。软件上的缺陷，如远程溢出，微软 IE 和 Outlook 的自动执行漏洞等，需要软件厂商和用户共同配合，不断地升级软件。而人为的缺陷，主要指的是计算机用户的疏忽。例如，当收到一封求职信邮件的时候，大多数人都会抱着好奇心去点击的。

企业防治蠕虫病毒主要考虑如下几个问题。

(1) 对用户进行安全培训。要及时对用户进行安全培训，提醒用户使用具有实时监控功能的杀毒软件，并且注意不要轻易打开、运行不明来源的文件。上网要尽量选择一些大的门户网站，尽量少上一些小且不知名的网站。对于来历不明的电子邮件，最好不要打开，尤其是附件。机器的安全设置可以设置得高一些，比如 IE 的安全级别可以设置为“中”，把其中所有 ActiveX 插件以及 Java 相关控件全部选择“禁用”。

(2) 及时更新系统安全补丁。由于蠕虫病毒是利用系统漏洞进行攻击，所以需要在第一时间保持系统和应用软件的安全性，保持各种操作系统和应用软件的及时更新，及时下载安装系统安全补丁。

(3) 部署网络防病毒系统。这方面主要依靠的是专业的计算机病毒防护系统，例如网络版的杀病毒软件 Symantec AntiVirus、瑞星等。通过它们可以在第一时间在整个网络内检测到网络异常和病毒攻击。

(4) 建立应急响应系统。由于蠕虫病毒爆发的突然性，可能在病毒发现的时候已经蔓延到了整个网络，所以在突发情况下，建立一个紧急响应系统是很有必要的，在病毒爆发的第一时间即能提供解决方案。

(5) 建立灾难备份系统。对于数据库和服务器数据系统，必须采用定期备份或多机备份措施，防止发生意外灾难时造成的数据丢失。

(6) 把本地的带有破坏性的程序更名。有些网络蠕虫病毒会通过调用系统中已经编译好的带有破坏性的程序来实现其功能。如果将本地的带有破坏性的程序改名字，比如把 format.com 改成 fmt.com，那么病毒的编辑者就无法用调用本地命令来实现这一功能。

(7) 更名或删除脚本程序的系统支持文件。由于蠕虫病毒大多是用 VBScript 脚本语言编写的，而 VBScript 代码是通过 Windows Script Host 来解释执行的，因此将 Windows Script Host 删除，就再也不用担心这些用 VBS 和 JS 编写的病毒了。Windows Script Host 本来是被系统管理员用来配置桌面环境和提供系统服务，实现最小化管理的一个手段，但对于大部分用户而言，WSH 并没有多大用处，所以普通用户可以禁止 Windows Script Host；也可以到 C:\Windows\System32 目录下，找到 WScript.exe 等脚本程序的系统支持文件，更改其名称或者干脆删除(这种做法有一定的副作用，如果删除脚本程序的系统支持文件，网页的 JS、WS 和 VBS 等脚本将不能再执行，所以应慎用)。

(8) 把邮件存放在其他分区。由于操作系统通常安装在 C 盘分区中，而且 C 盘又是启动分区，所以 C 盘往往是病毒攻击频率最高的地方。而且蠕虫病毒最常用的入侵途径就是邮件。而按系统默认的设置，一般微软的 OE(Outlook Express)邮件存放的位置是系统安装分区(通常是 C 盘)，这样就会使 C 盘分区受到蠕虫攻击的可能性再度提高，使系统安全受到严重威胁。所以建议把 OE 中的邮件存放位置改在其他非系统、非启动分区中。

2.5　狙击波蠕虫病毒防护

2.5.1　狙击波蠕虫病毒概述

狙击波蠕虫病毒(Worm. Zotob)是 2005 年以来最早利用微软漏洞攻击计算机的蠕虫病毒，该病毒最初可能源自欧洲芬兰，之后在欧洲迅速流传。到 2005 年 8 月 18 日美国部分重要企业和政府机构遭受此次蠕虫狂潮的袭击，并造成网络瘫痪。但该蠕虫病毒在中国内地并未出现大规模泛滥。从截获的“狙击波”及其变种分析，最主要的原因是狙击波及其变种均为国外作者编写，可完全攻击和感染英文版的 Windows 系统。所以对于中文 Windows 系统，该病毒虽然可以攻击计算机并导致计算机重启，却不能致使其感染。

狙击波是 Windows 下的 PE 病毒，利用了微软公布的严重系统漏洞，即 Windows Plug and Play(即插即用)中存在的漏洞(MS05-039)。Plug and Play 中存在 Windows 未经检查的缓冲区，成功利用此漏洞的攻击者可以控制受影响的系统。和冲击波、震荡波方法类似，攻击代码向目标系统的 TCP 445 端口发送漏洞代码，使目标系统造成缓冲区溢出，同时运行病毒代码，以进行传播。

病毒在系统中成功执行后，将进行以下的三个操作：

(1) 病毒启动后，会将自己复制到系统目录中，病毒文件名为 botzor. exe。

(2) 在注册表中添加下列启动项。

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Currentversion\Run
"WINDOWS SYSTEM"=botzor.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Currenversion\RunServices
"WINDOWS SYSTEM"=botzor.exe
```

(3) 在感染的时候，病毒利用 IP 扫描的方式在网络中寻找具有漏洞的系统，发现后就会对系统进行攻击，先连接系统的 TCP 445 端口，并植入系统中一个远程 SHELL，此远程 SHELL 释放一个文件 2PAC. TXT，此文件中包含有一段 FTP 命令脚本，功能是利用 FTP 从远程将病毒文件下载到本地。

(4) 如果攻击失败，则造成类似冲击波、震荡波引起的计算机重启。

(5) 修改系统的 HOST 文件，添加造成用户不能访问杀毒软件网站的内容，使相关杀毒软件不能升级。

2.5.2　狙击波蠕虫病毒防护步骤

根据狙击波蠕虫病毒的原理，狙击波是通过 TCP 的 445 端口实施攻击的，因此，封闭



TCP 445 端口是最好的病毒预防方法。具体的方法非常多,如通过防火墙封锁、Windows 高级 TCP/IP 设置中的 IP 筛选器、修改注册表等。在这里,通过本地安全策略封闭 TCP 445 端口,以学习如何预防狙击波,并认识在 Windows 系统下自定义封闭端口或者禁止 ICMP 数据的方式。

(1) 选择【控制面板】/【管理工具】/【本地安全设置】/【安全设置】选项,右击【IP 安全策略,在本地计算机】,选择【管理 IP 筛选器表和筛选器操作】命令,如图 2-63 所示。



图 2-63 【本地安全设置】窗口

(2) 在打开的【管理 IP 筛选器表和筛选器操作】对话框中,单击【添加】按钮,如图 2-64 所示。



图 2-64 【管理 IP 筛选器表和筛选器操作】对话框

(3) 在弹出的【IP 筛选器列表】对话框中,取消选择【使用“添加向导”】复选框,单击【添





加】按钮，如图 2-65 所示。

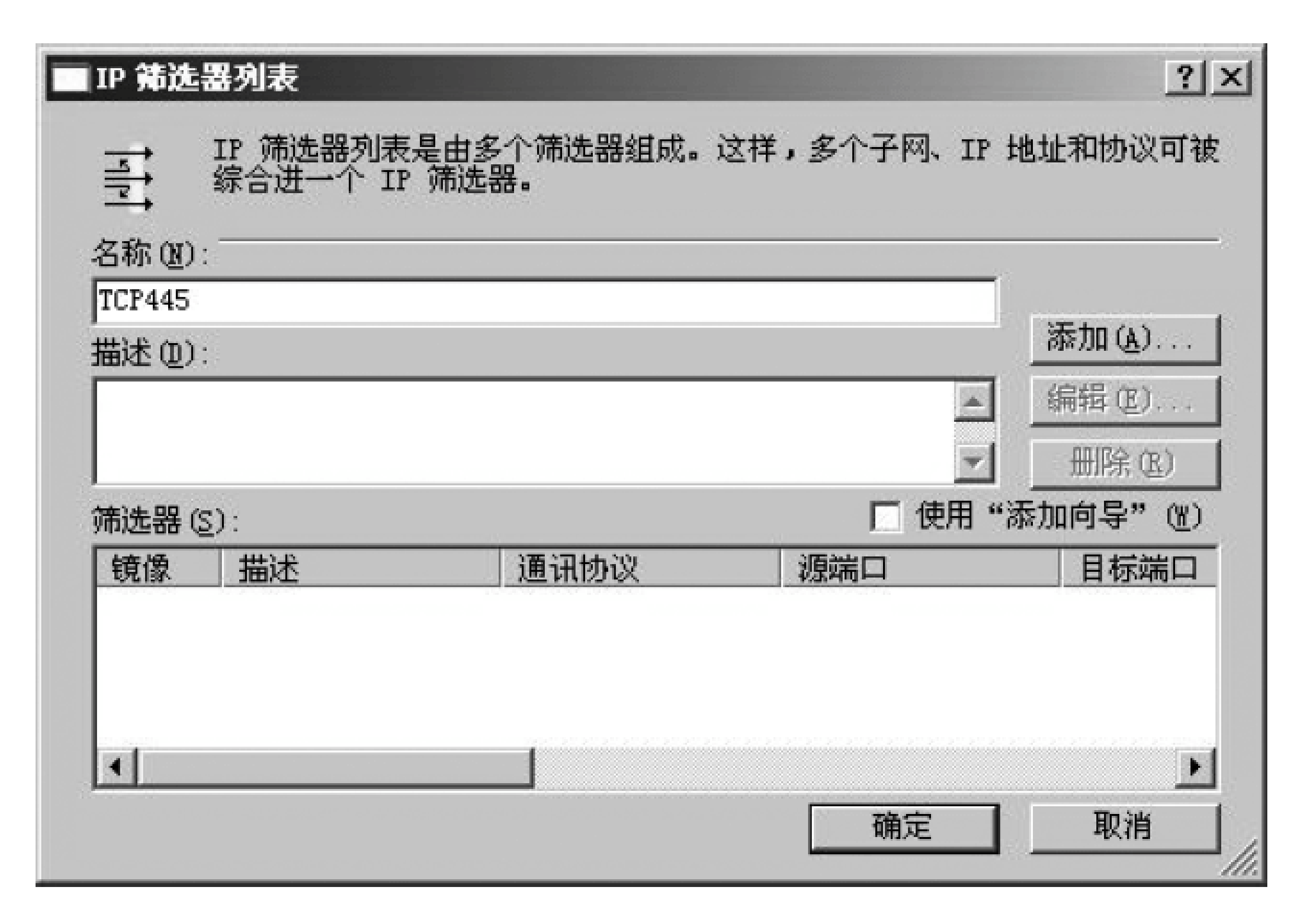


图 2-65　【IP 筛选器列表】对话框

(4) 接着弹出【筛选器 属性】对话框，在【寻址】选项卡中，选择【源地址】为“任何 IP 地址”，【目标地址】为“我的 IP 地址”，如图 2-66 所示。

(5) 选择【协议】选项卡，设置【选择协议类型】为 TCP，【到此端口】设置为 445，如图 2-67所示。



图 2-66　【寻址】选项卡

图 2-67　【协议】选项卡

提示：读者可以根据上述步骤学习封闭其他端口，甚至禁止某些协议通信。

(6) 单击【确定】按钮，回到【IP 筛选器列表】对话框，再单击【确定】按钮。回到【管理 IP 筛选器表和筛选器操作】对话框后，最后单击【确定】按钮，完成筛选器的添加。

(7) 接下来是添加应用此筛选器的 IP 策略。回到【本地安全设置】窗口后，同样右击【IP 安全策略，在本地计算机】，选择【创建 IP 安全策略】命令。



(8)进入【IP 安全策略向导】对话框后,单击【下一步】按钮,接着输入策略名称,同样使用 TCP445,如图 2-68 所示。

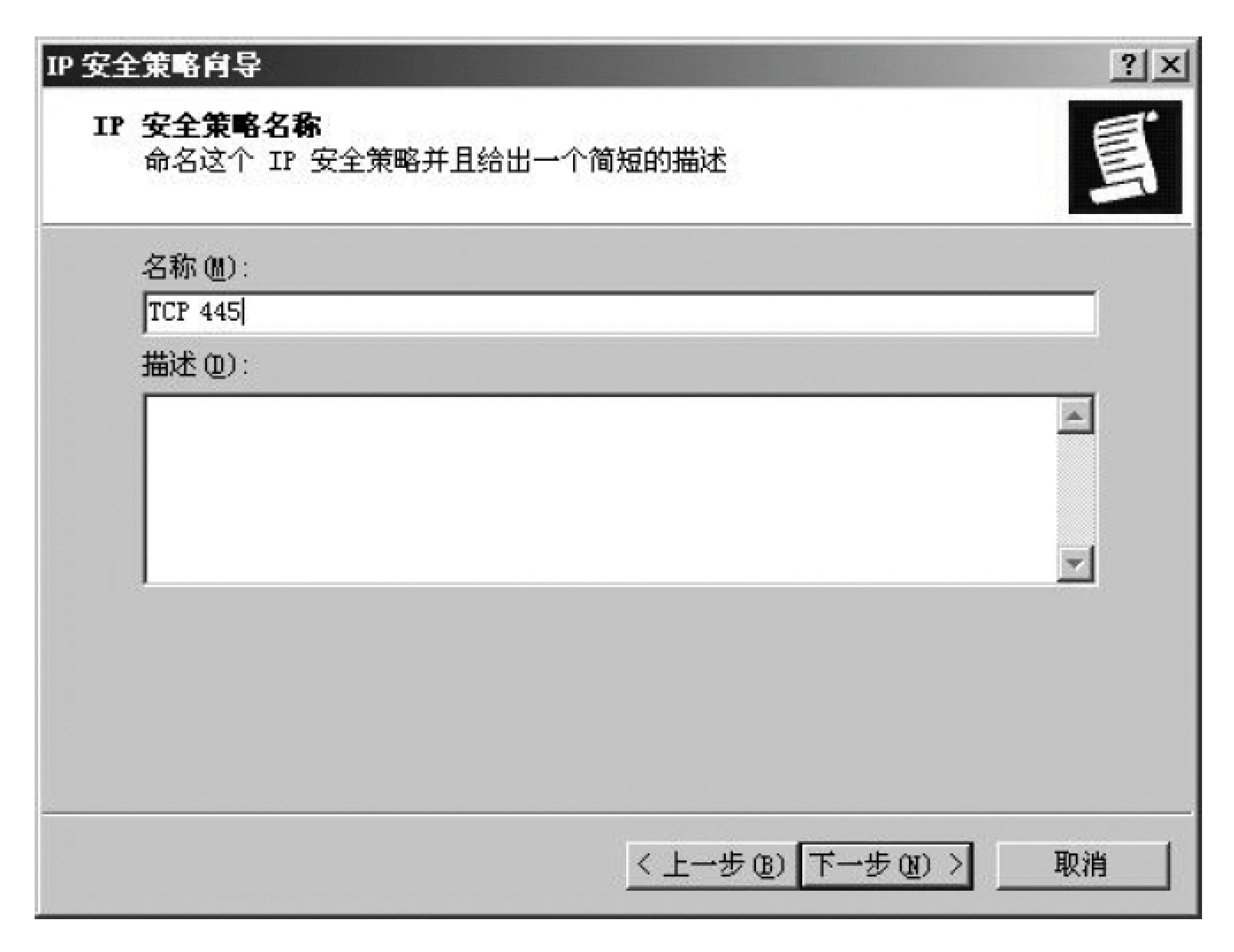


图 2-68 【IP 安全策略名称】对话框

(9)单击【下一步】按钮,进入【安全通信请求】对话框,取消选中【激活默认响应规则】复选框,单击【下一步】按钮,再单击【完成】按钮,如图 2-69 所示。

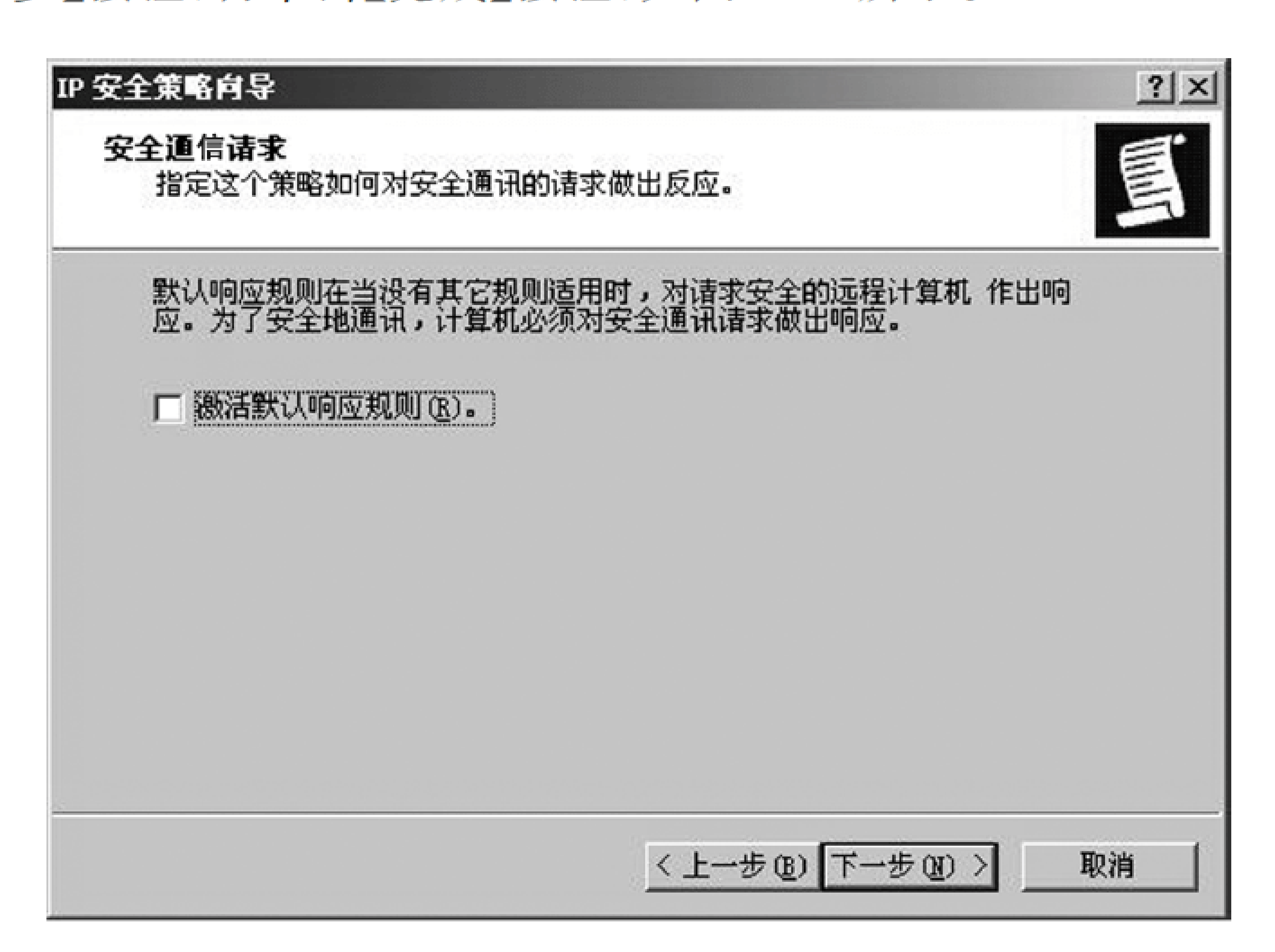


图 2-69 【安全通信请求】对话框

(10)接着对该 IP 安全策略进行属性设置,在【TCP 445 属性】对话框中,取消【使用"添加向导"】的选择,然后单击【添加】按钮,如图 2-70 所示。

(11)出现【新规则 属性】对话框,在【IP 筛选器列表】中选择刚才定义的筛选器,如图 2-71所示。

(12)选择【筛选器操作】标签,同样去掉【使用"添加向导"】复选框的选中状态,单击【添加】按钮,如图 2-72 所示。



(13) 在弹出的【新筛选器操作 属性】对话框的【安全措施】选项卡中，选择【阻止】单选按钮，单击【确定】按钮退出，如图 2-73 所示。



图 2-70　【规则】选项卡

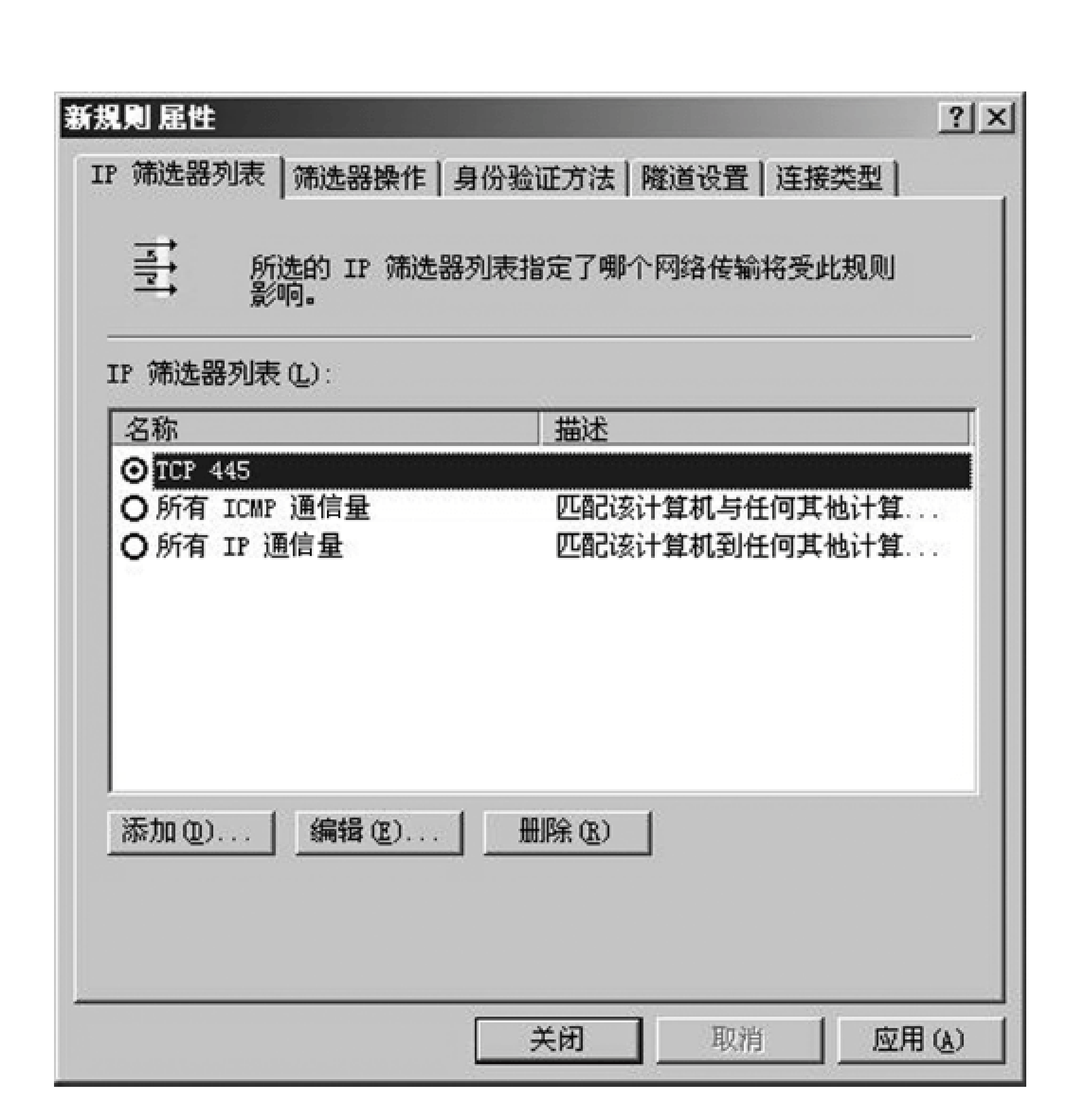


图 2-71　选择筛选器



图 2-72　【筛选器操作】选项卡

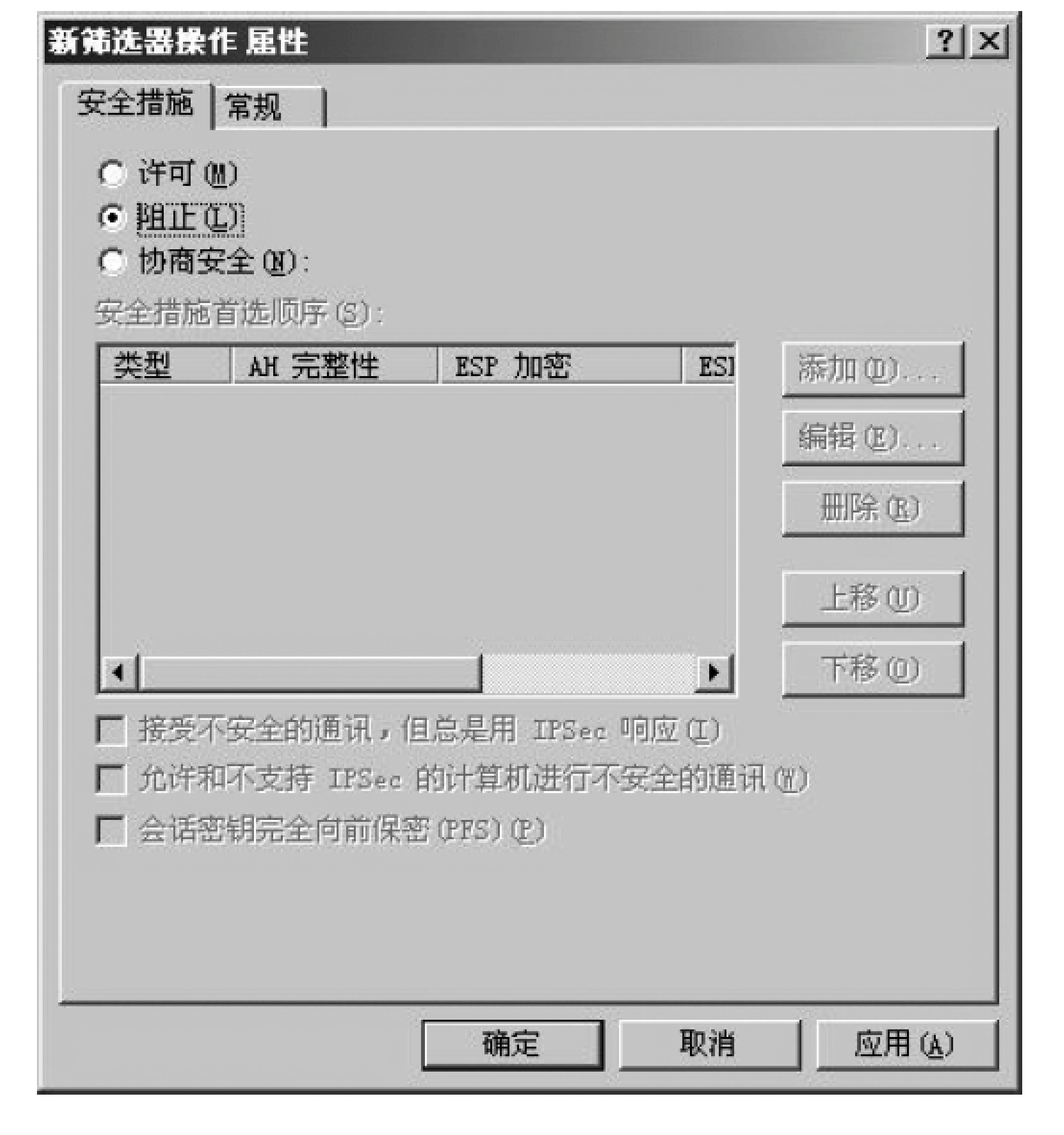


图 2-73　筛选器操作规则

(14) 回到【新规则 属性】对话框，在【筛选器操作】选项卡中选择刚才定义的"筛选器操作"，然后单击【确定】按钮，退出对话框。

(15) 回到【TCP 445 属性】对话框，单击【确定】按钮退出，此时发现【本地安全设置】中已经添加了新策略 TCP 445。右击此策略，选择【指派】命令，这样，该策略将应用到系统中，本地的 445 端口将禁止一切的通信，如图 2-74 所示。





图 2-74　设置完成

(16) 在任务栏中选择【开始】/【运行】命令，打开【运行】对话框，在文本框中输入 gpupdate 命令，单击【确定】按钮，更新本地安全策略，如图 2-75 所示。



图 2-75　更新本地安全策略

通过上述方法，可以有效地避免狙击波病毒的感染。

提示：可以使用端口扫描工具扫描计算机，查看 TCP 445 端口是否可以通信。

2.6　木　　马

木马也是目前最主要的网络安全威胁之一，而且因为它是近几年发展起来的，所以目前许多杀病毒软件对木马的查杀能力比较有限，清除木马的难度更大。

2.6.1　木马概述

“木马”的全名为“特洛伊木马”，英文叫做“Trojan Horse”，是一种基于客户机和服务器(C/S)模式的远程控制程序。其名称取自希腊神话的特洛伊木马记。希腊人围攻特洛伊城，久久不能得手，后来想出了一个木马计，让士兵藏匿于巨大的木马中。大部队假装撤退而将木马摈弃于特洛伊城，让敌人将其作为战利品拖入城内。木马内的士兵则乘夜晚敌人庆祝胜利、放松警惕的时候从木马中爬出来，与城外的部队里应外合而攻下了特洛伊城。后来，人们就常用“特洛伊木马”这一典故，用来比喻在敌方营垒里埋下伏兵、里应外合的活动。

大多数木马包括客户端和服务器端两个部分。攻击者利用一种称为绑定程序的工具将服务器绑定到某个合法软件上，只要用户一运行被绑定的合法软件，木马的服务器部分就在



用户毫不知情的情况下完成了安装过程。通常，木马的服务器部分都是可以定制的，攻击者可以定制的项目一般包括服务器运行的 IP 端口号、程序启动时机、如何发出调用、如何隐身、是否加密。另外，攻击者可以设置登录服务器的密码，确定通信方式。木马攻击者既可以随心所欲地查看已被入侵的机器，也可以用广播方式发布命令，指示所有在他控制之下的木马一起行动，或者向更广泛的范围传播，或者做其他危险的事情。

木马的设计者为了防止木马被发现，会采用多种手段隐藏木马，这样用户即使发现感染木马，也很难找到并清除它。木马的危害越来越大，保障安全的最好方法就是熟悉木马的类型、工作原理，掌握如何检测和预防这些代码。常见的木马，例如冰河、灰鸽子和 BO2K (Back Orifice)等，都是多用途的攻击工具包，功能非常全面，包括捕获屏幕、声音、视频内容的功能。这些木马可以当作键记录器、远程控制器、FTP 服务器、HTTP 服务器、Telnet 服务器，还能够寻找和窃取密码。攻击者可以配置木马监听的端口、运行方式，以及木马是否通过 E-mail、QQ、ICQ、IRC(Internet Relay Chat，互联网中继聊天)或其他通信手段联系发起攻击的人。一些危害大的木马还有一定的反侦探能力，能够采取各种方式隐藏自身，加密通信，甚至提供了专业级的 API 供其他攻击者开发附加功能。

2.6.2　木马的组成

一个完整的木马系统由硬件部分、软件部分和网络连接三部分组成。

1. 硬件部分

建立木马连接所必需的硬件实体，包括服务器端、控制端和连接服务器端与控制端的网络。服务器端是被控制端远程控制的目标计算机，是安装了木马程序的服务器端；控制端是对服务器端进行远程控制的计算机，是安装了木马程序的客户端；而网络则是控制端对服务器端进行远程控制、数据传输的网络载体。

2. 软件部分

软件部分是实现远程控制所必需的程序。与硬件部分对应，它分为服务器端程序、控制端程序和木马配置程序三部分。图 2-76 所示是著名木马 BO2K 的程序。服务器端程序就是木马系统的服务器程序，它被隐藏安装在目标计算机内部，以获取对目标计算机的操作权限和其他所需的信息；而控制端程序就是客户端程序，是用来与远程服务器端连接，并控制服务器端行为的客户端程序；木马配置程序是设置木马程序的端口号、触发条件、木马名称等，使其在服务器端藏得更隐蔽的程序。

3. 网络连接

木马系统通过网络连接可在服务器端和控制端之间建立一条木马通信通道，为服务器端发送所获取的信息，控制端发出控制指令提供通道。木马攻击是通过网络进行的，可以是局域网，也可以是 Internet 之类的广域网。但多数还是通过 Internet 进行的，具体的网络连接方式没有限制，只要有通道即可。



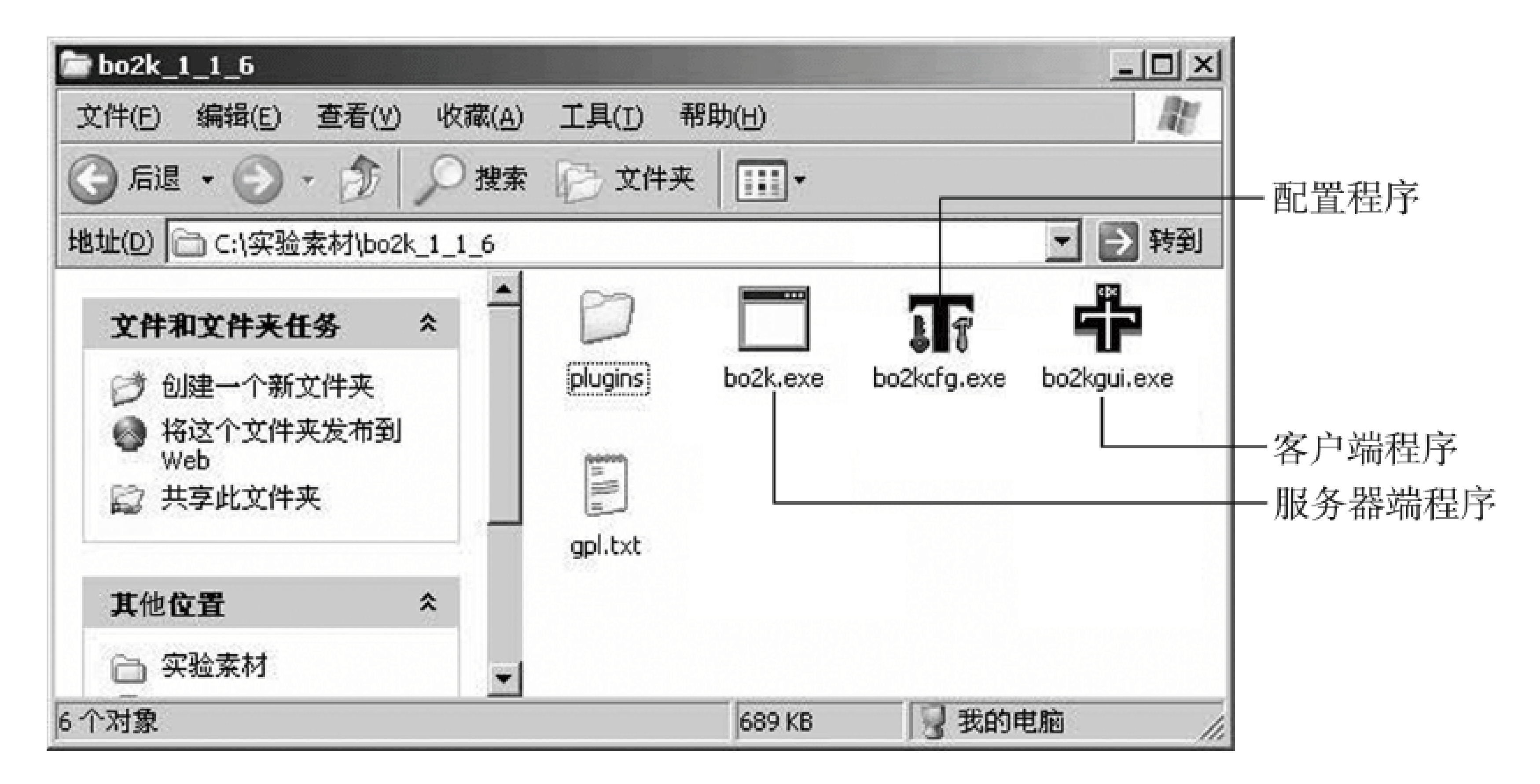


图 2-76　木马程序的组成

2.6.3　木马的攻击原理

黑客用木马进行网络入侵，从过程上看大致可分为六步，下面从这六步来详细阐述木马的攻击原理。

1. 配置木马

一般来说，一个设计成熟的木马都有木马配置程序，从具体的配置内容看，主要是为了实现以下两方面功能：

（1）木马伪装。木马配置程序为了在服务器端尽可能好地隐藏木马，会采用多种伪装手段，如修改图标、捆绑文件、定制端口、自我销毁等。

（2）信息反馈。木马配置程序将就信息反馈的方式或地址进行设置，如设置信息反馈的 E-mail、IRC 号和 QQ 号等。

2. 传播木马

（1）传播方式。木马的传播方式主要有两种：一种是通过电子邮件，即控制端将木马程序以附件的形式夹在邮件中发送出去，收信人只要打开附件系统就会感染木马；另一种是软件下载，即一些非正规的网站以提供软件下载为名义，将木马捆绑在软件安装程序上，下载后，只要一运行这些程序，木马就会自动安装。

（2）伪装与隐藏方式。木马设计者为了使自己所设计的木马程序不轻易被人发现，往往在开发时采用多种方式来伪装木马，以达到降低用户警觉、欺骗用户的目的。其形式主要有以下几种。

① 在任务栏中隐藏。这是最基本的方法，只要在设计木马程序时把 Form 的 Visible 属性设为 False、ShowInTaskBar 属性设为 False，木马程序运行时就不会出现在任务栏中。

② 在任务管理器中隐形。将木马程序设为“系统服务”，伪装为系统的一部分。

③ 修改图标。现在已经有木马可以将木马服务器端程序的图标改成 HTML、TXT、ZIP 等各种文件的图标，具有相当大的迷惑性。当用户在邮件的附件中看到这种常见文件

类型的图标时，很有可能就是一个木马程序。

④ 捆绑文件。这种伪装手段是将木马捆绑到一个安装程序上，当安装程序运行时，木马在用户毫无察觉的情况下，偷偷地进入了系统。被捆绑的文件一般是可执行文件，如EXE、COM 等文件。

⑤ 出错显示。有些木马提供了出错显示功能。当服务器端用户打开木马程序时，会弹出一个假的错误提示框，错误内容可自由定义，大多会定制成一些诸如"文件已破坏，无法打开的！"之类的信息，当服务器端用户信以为真时，木马却悄悄侵入了系统。

⑥ 定制端口。很多老式的木马端口都是固定的，这给判断是否感染了木马带来了方便，只要查一下特定的端口就知道感染了什么木马，所以现在很多新式的木马都加入了定制端口的功能，控制端用户可以在 1024～65 535 之间任选一个端口作为木马端口（一般不选 1024 以下的端口），这样就给判断所感染木马类型带来了麻烦。

⑦ 自我销毁。当服务器端用户打开含有木马的文件后，木马一般会将自己复制到 Windows 的系统文件夹（C:\Windows 或 C:\Windows\System）中。而木马的自我销毁功能是指安装完木马后，原木马文件将自动销毁，这样服务器端用户就很难找到木马的来源，在没有查杀木马的工具帮助下，就很难删除木马了。

⑧ 木马更名。安装到系统文件夹中的木马文件名一般是固定的，只要根据一些查杀木马的文件，在系统文件夹查找特定的文件，就可以断定中了什么木马。但是，现在有很多木马都允许控制端用户自由定制安装后的木马文件名，这样给判断是否感染了木马以及所感染木马的类型带来困难。

目前除了上面介绍的隐身技术外，更隐蔽的方法已经出现，那就是驱动程序及动态链接库技术。驱动程序及动态链接库技术和一般的木马不同，它基本上摆脱了原有的木马模式——监听端口，而采用替代系统功能的方法（改写驱动程序或动态链接库）。这样做的结果是：系统中没有增加新的文件（所以不能用扫描的方法查杀），不需要打开新的端口（所以不能用端口监视的方法查杀），没有新的进程（所以使用进程查看的方法发现不了它，也不能用杀掉进程的方法终止它的运行）。在正常运行时木马几乎没有任何的症状，而一旦木马的控制端向被控制端发出特定的信息后，隐藏的程序就立即开始运作。

3. 运行木马

服务器端用户运行木马或捆绑木马的程序后，木马就会自动进行安装。首先将自身复制到 Windows 的系统文件夹中，然后在注册表、启动组、非启动组中设置好木马的触发条件，这样木马的安装就完成了。安装后就可以运行木马了，具体过程如下。

(1) 木马的触发条件。触发条件是指启动木马的条件，大致有如下几个方面：

① 注册表。木马程序通常在注册表的 Run、RunOnce 和 RunServices 主键中，如图 2-77 所示。可以在其中寻找可能是启动木马的键值。

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
```

图 2-77　注册表的 Run 主键



② win.ini 文件。打开系统配置文件 win.ini，在[windows]字段中有启动命令 load=和 run=，在一般情况下是空白的，如果有启动程序，可能是木马。

③ system.ini 文件。在系统配置文件 system.ini 的 [386Enh]、[mci]、[drivers32]字段中有命令行，在其中可能会找到木马的启动命令。

④ Autoexec.bat 和 Config.sys 文件。在 C 盘根目录下的这两个文件也可以启动木马。但这种加载方式一般都需要控制端用户与服务器端建立连接后，将已添加木马启动命令的同名文件上传到服务器端覆盖这两个文件才行。

⑤ 其他.ini 文件。.ini 文件是应用程序的启动配置文件，控制端利用这些文件能启动程序的特点，将制作好的带有木马启动命令的同名文件上传到服务器端覆盖这同名文件，这样就可以达到启动木马的目的了。

⑥ 启动菜单。在【开始】/【程序】/【启动】中的菜单项也可能是木马的触发条件，不过这种方式最容易被发现，一般攻击者不会使用。

⑦ 捆绑文件。实现这种触发条件首先要控制端和服务器端已通过木马建立连接，然后控制端用户用工具软件将木马文件和某一应用程序捆绑在一起，然后上传到服务器端覆盖原文件，这样即使木马被删除了，只要运行捆绑了木马的应用程序，木马又会被安装上去。

⑧ 自动播放。自动播放本是用于光盘的，当插入一个电影光盘到光驱时，系统会自动播放里面的内容，这就是自动播放的本意，播放什么是由光盘中的 AutoRun.inf 文件指定的，修改 AutoRun.inf 中的 open 一行可以指定在自动播放过程中运行的程序。后来有人用于硬盘与 U 盘，在 U 盘或硬盘的分区，创建 Autorun.inf 文件，并在 Open 中指定木马程序，这样，当打开硬盘分区或 U 盘时，就会触发木马程序的运行。

(2) 木马运行过程。木马被激活后，进入内存，并开启事先定义的木马端口，准备与控制端建立连接。这时服务器端用户可以在 MS-DOS 方式下，输入 netstat-an 命令查看端口状态。一般个人计算机在脱机状态下是不会有端口开放的，如果有端口开放，就要注意是否感染木马了。

不过，现在互联网应用非常多了，在上网过程中要下载软件、发送信件、网上聊天等，必然会打开一些端口。注意这些互联网应用软件所用的端口对于区别是否中了木马非常有用。如 1～1024 端口称为“保留端口”，是专用于系统常见服务的。如 FTP 使用 21，SMTP 使用 25，POP3 使用 110 等。木马一般不会使用这些端口，因为这些保留端口在系统启动时已给相应的服务占用了。

另外，如 4000～4001 端口是 QQ 的通信端口，6667 端口是 IRC 的通信端口。

除上述的端口外，如发现还有其他端口打开，尤其是数值比较大的端口，那就要怀疑是否感染了木马。当然如果木马有定制端口的功能，那任何端口都有可能是木马端口。

4. 盗取信息

一般来说，设计成熟的木马都有一个信息反馈机制。所谓信息反馈机制，是指木马成功安装后会收集一些服务器端的软硬件信息，并通过 E-mail、IRC、QQ 或 ICQ 的方式告知控制端用户。

控制端从反馈信息中可以知道服务器端的一些软硬件信息，包括使用的操作系统、系统目录、硬盘分区状况、系统口令等，在这些信息中，最重要的是服务器端 IP 地址，因为只有得

到这个参数,控制端才能与服务器端建立连接。

5. 建立连接

一个木马连接的建立首先必须满足两个条件：一是服务器端已安装了木马程序;二是控制端、服务器端都要在线。在此基础上控制端可以通过木马端口与服务器端建立连接。

假设A机为控制端,B机为服务器端,对于A机来说要与B机建立连接,必须知道B机的木马端口和IP地址。由于木马端口是A机事先设定的,为已知项,所以最重要的是如何获得B机的IP地址。获得B机的IP地址的方法主要有两种：信息反馈和IP扫描。由于扫描整个IP地址段既费时又费力,一般来说控制端都是通过信息反馈获得服务器端的IP地址。

6. 远程控制

木马连接建立后,控制端端口和木马端口之间将会出现一条通道。控制端程序可依靠这条通道与服务器端上的木马程序取得联系,并通过木马程序对服务器端进行远程控制,获取对服务器端的控制权。

2.6.4　木马的危害

黑客通过木马程序获取对服务器端的控制权后,可实施的危害行为主要有如下几种：

(1) 窃取密码。一切以明文的形式或缓存在Cache中的密码都能被木马侦测到,此外很多木马还提供击键记录功能,它将会记录服务器端每次敲击键盘的动作,所以一旦有木马入侵,密码将很容易被窃取。

(2) 文件操作。控制端可依靠远程控制对服务器端的文件进行删除、新建、修改、上传、下载、运行、更改属性等一系列操作,基本涵盖了Windows平台上所有的文件操作功能。

(3) 修改注册表。控制端可任意修改服务器端注册表,包括删除、新建或修改主键、子键和键值。有了这项功能,控制端就可以禁止服务器端软驱、光驱的使用,锁住服务器端的注册表,将服务器端上木马的触发条件设置得更隐蔽等。

(4) 系统操作。这项内容包括重启或关闭服务器端操作系统,断开服务器端网络连接,控制服务器端的鼠标、键盘,监视服务器端桌面操作,查看服务器端进程等,控制端甚至可以随时给服务器端发送信息。

2.6.5　木马的识别和清除

1. 检查木马

知道了木马的攻击原理和隐身方法,就可以采取以下措施进行防御。

(1) 端口扫描。端口扫描是检查远程机器有无木马的最好办法。端口扫描的原理非常简单,扫描程序尝试连接某个端口,如果成功,则说明端口开放;如果失败或超过某个特定的时间(超时),则说明端口关闭。但对于驱动程序/动态链接库木马,扫描端口是不起作用的。

(2) 查看连接。查看连接和端口扫描的原理基本相同,不过是在本地机器上通过运行netstat-an命令(或某个第三方程序)查看所有的TCP/UDP连接,查看连接要比端口扫描



快，但同样是无法查出驱动程度/动态链接库木马，而且仅仅能在本地使用。

(3) 检查注册表。木马可以通过注册表启动(好像现在大部分的木马都是通过注册表启动的，至少也把注册表作为一个自我保护的方式)，那么，同样可以通过检查注册表来发现木马在注册表里留下的痕迹。

(4) 查找文件。查找木马特定的文件也是一个常用的方法，如“冰河”木马的特征文件是 kernel32.exe 和 sysexlpr.exe，只要删除这两个文件，木马就已经不起作用了。

另外，对于驱动程度/动态链接库木马，有一种方法可以尝试，使用 Windows 的“系统文件检测器”，通过【开始】/【程度】/【附件】/【系统工具】/【系统信息】/【工具】可以运行【系统文件检查器】，用【系统文件检查器】可检测操作系统文件的完整性。如果这些文件损坏，检查器可以将其还原，检查器还可以从安装盘中解压缩已压缩的文件(如驱动程序)。如果驱动程序或动态链接库在没有升级的情况下被改动了(或者被损坏了)，就有可能是木马，提取改动过的文件可以保证系统的安全和稳定。

2. 预防和清除木马

(1) 木马的预防。针对那些已知使用特定端口的木马，用户可以采取关闭其所使用端口的方法，达到预防木马入侵的目的。可以利用“本地安全策略”关闭特定端口，详细步骤参考 2.5 节。

(2) 木马的清除。根据木马的攻击原理，可以手工清除木马，但是大多数用户都是通过各种杀毒软件、木马专杀工具进行木马查杀的。

为了对付日益增加的木马攻击，普通的杀毒软件也加入了对木马的查杀，例如国内的三大品牌金山、瑞星、江民，国外的著名品牌诺顿、趋势、NOD32、卡巴斯基、AVG 等。

很多公司开发了专门针对木马的清除工具，其中比较著名的有 The Cleaner、木马克星、微软的 Malicious Software Removal Tool 等，专门用于清除包括木马在内的恶意软件。

2.7 木马的安装及使用

2.7.1 BO2K 概述

在国际上，木马程序中最著名的当属 BO2K(Back Orifice)，以多功能、代码简洁而著称。BO2K 程序主要分成以下三部分。

- bo2k.exe：这是服务器程序，它的作用是负责执行入侵者的命令。
- bo2kgui.exe：这是 BO2K 的客户端程序，其作用是用来控制服务器程序执行。
- bo2kcfg.exe：这是服务器设置程序，在使用 bo2k.exe 服务器程序之前，有一些相关的功能必须通过它来进行设置，如使用的 TCP/IP 端口、程序名称、密码等。

另外，BO2K 还支持插件功能，攻击者可以自己编写功能更强的插件来扩展 BO2K 的功能。

2.7.2　BO2K 安装与使用步骤

1. BO2K 的安装

BO2K 一般都是以压缩文件在网站(http://bo2k.sourceforge.net/)上发布的,下载并解压后,打开即可看到如图 2-78 所示的文件,包括服务器 bo2k.exe、服务器配置工具 bo2kcfg.exe、客户端 bo2kgui.exe。其子文件夹 plugins 内包含用于扩展服务器和客户端功能的插件。



图 2-78　BO2K 文件列表

2. 服务器端程序的配置

(1) 服务器端 IP 设置,如图 2-79 所示。

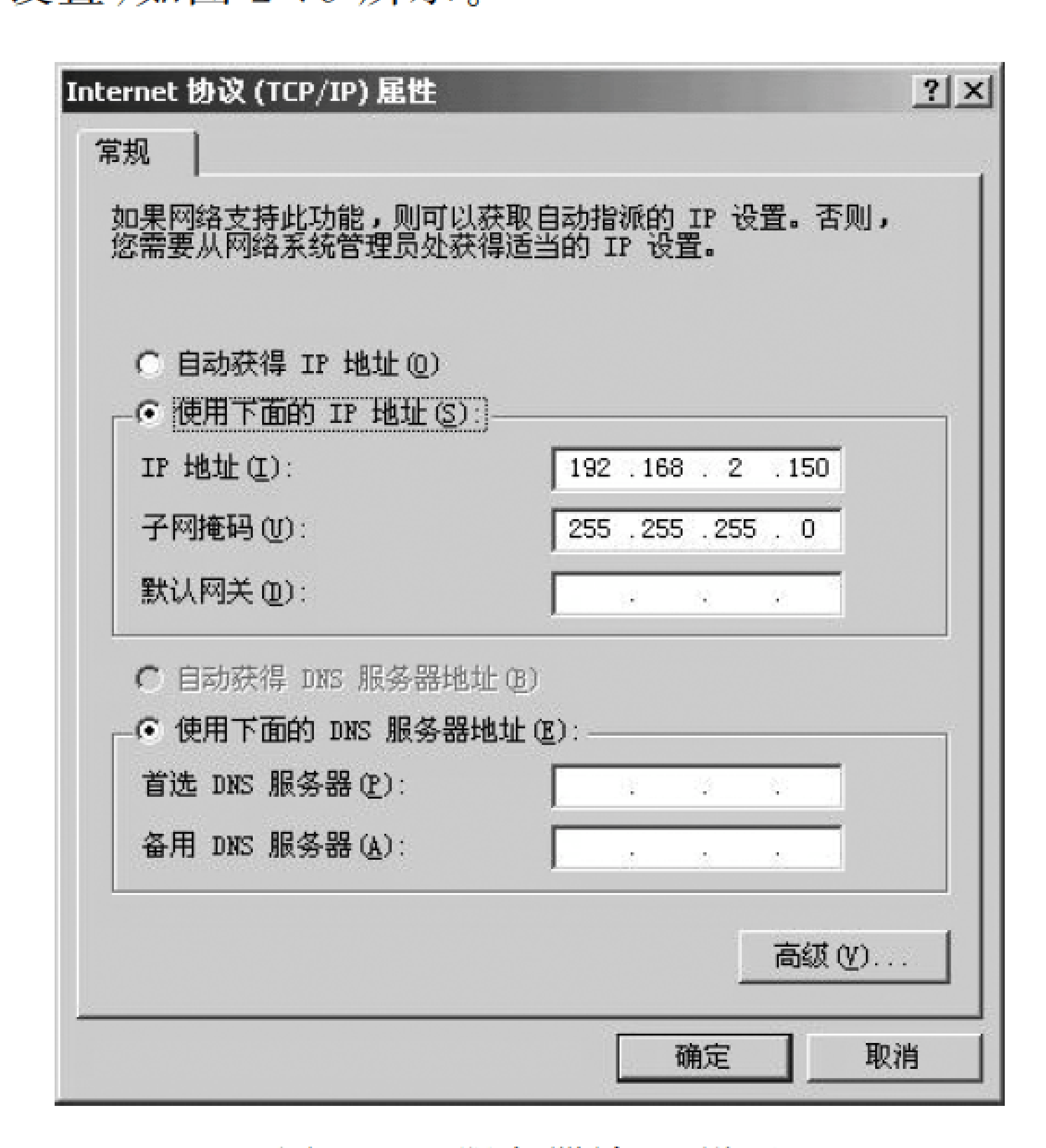


图 2-79　服务器端 IP 设置



(2) 启动 BO2K 的配置工具。运行 bo2kcfg.exe，单击 Open Server(打开服务器)按钮，输入要配置的服务器文件，选择图 2-78 中的 bo2k.exe，结果如图 2-80 所示。

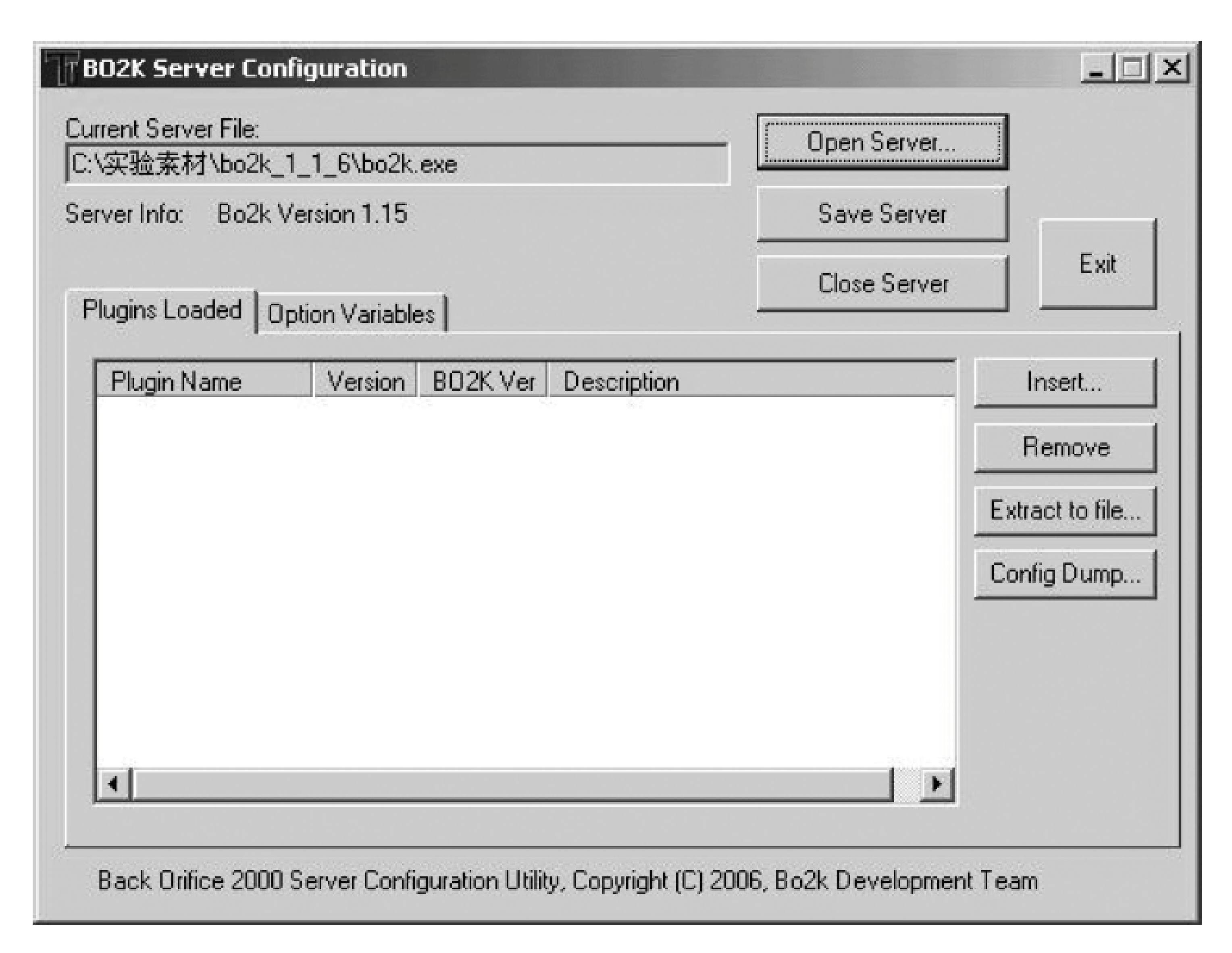


图 2-80　服务器文件配置

(3) 插件配置。单击 Insert(插入)按钮添加插件，插件放在如图 2-78 所示的 plugins 文件夹中，添加的插件包括 auth、enc、io、misc、srv 目录下的所有 DLL 文件，结果如图 2-81 所示。

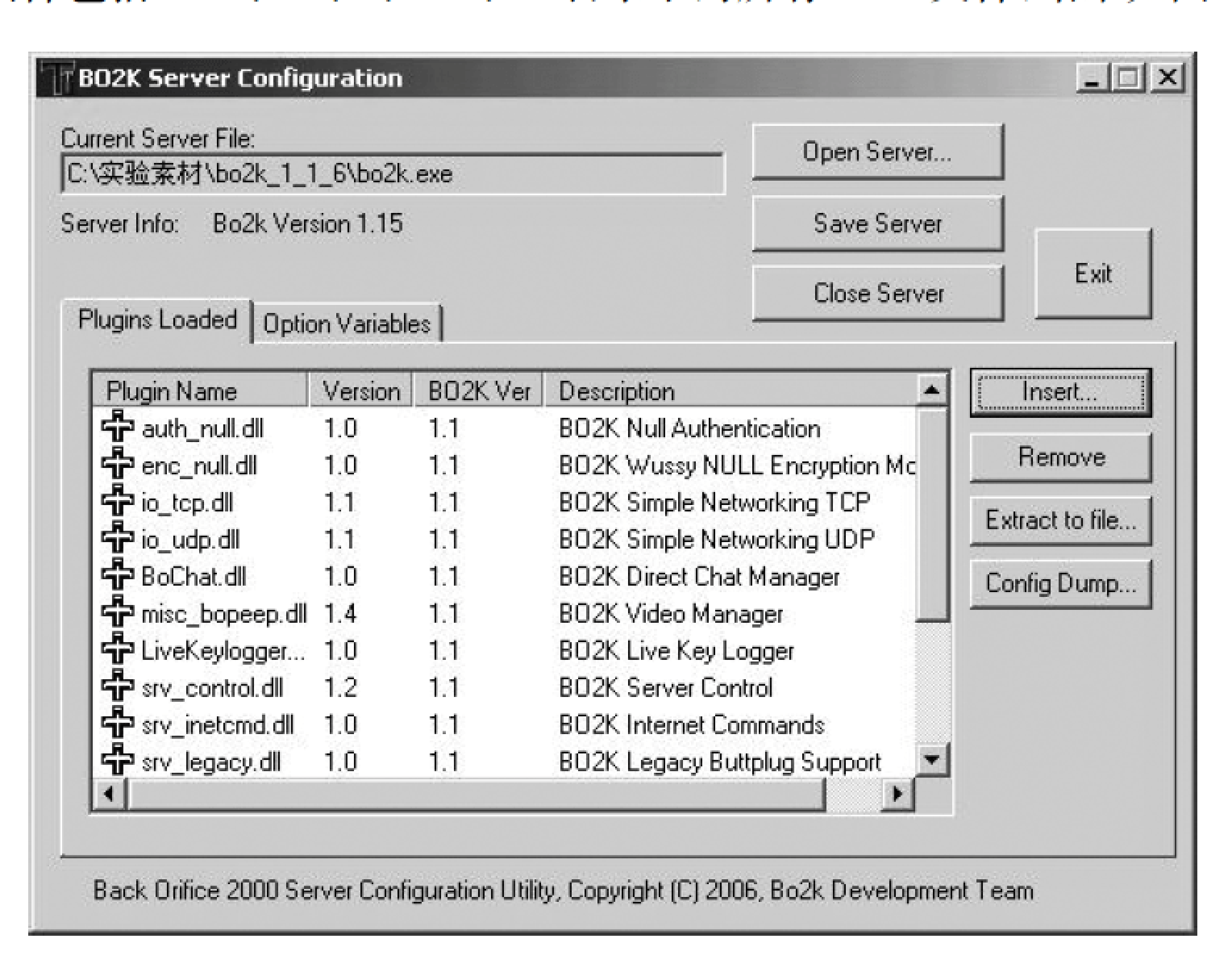


图 2-81　插件配置

(4) 服务器配置。单击 Option Variables(选择变量)标签，如图 2-82 所示，可以在此配置 BO2K 服务器所使用的网络通信方式、端口号、加密方法等。选择使用默认配置即可。

(5) 单击 Save Server(保存服务器)按钮保存配置信息，然后单击 Exit(退出)按钮退出配置程序。



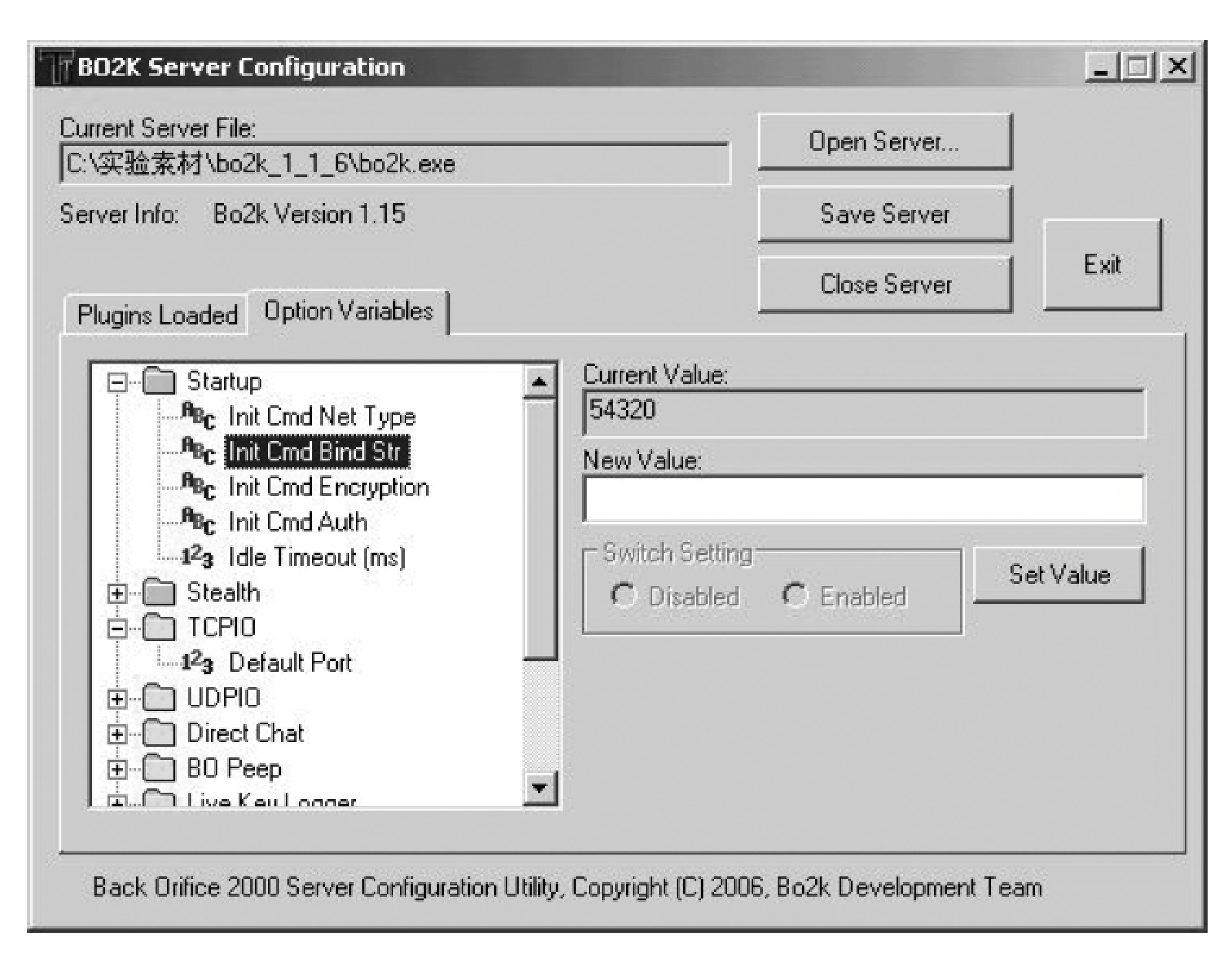


图 2-82　服务器配置

（6）双击 bo2k. exe 就可以运行服务器程序。

3. 客户端程序的使用

（1）客户端 IP 参数设置，如图 2-83 所示。

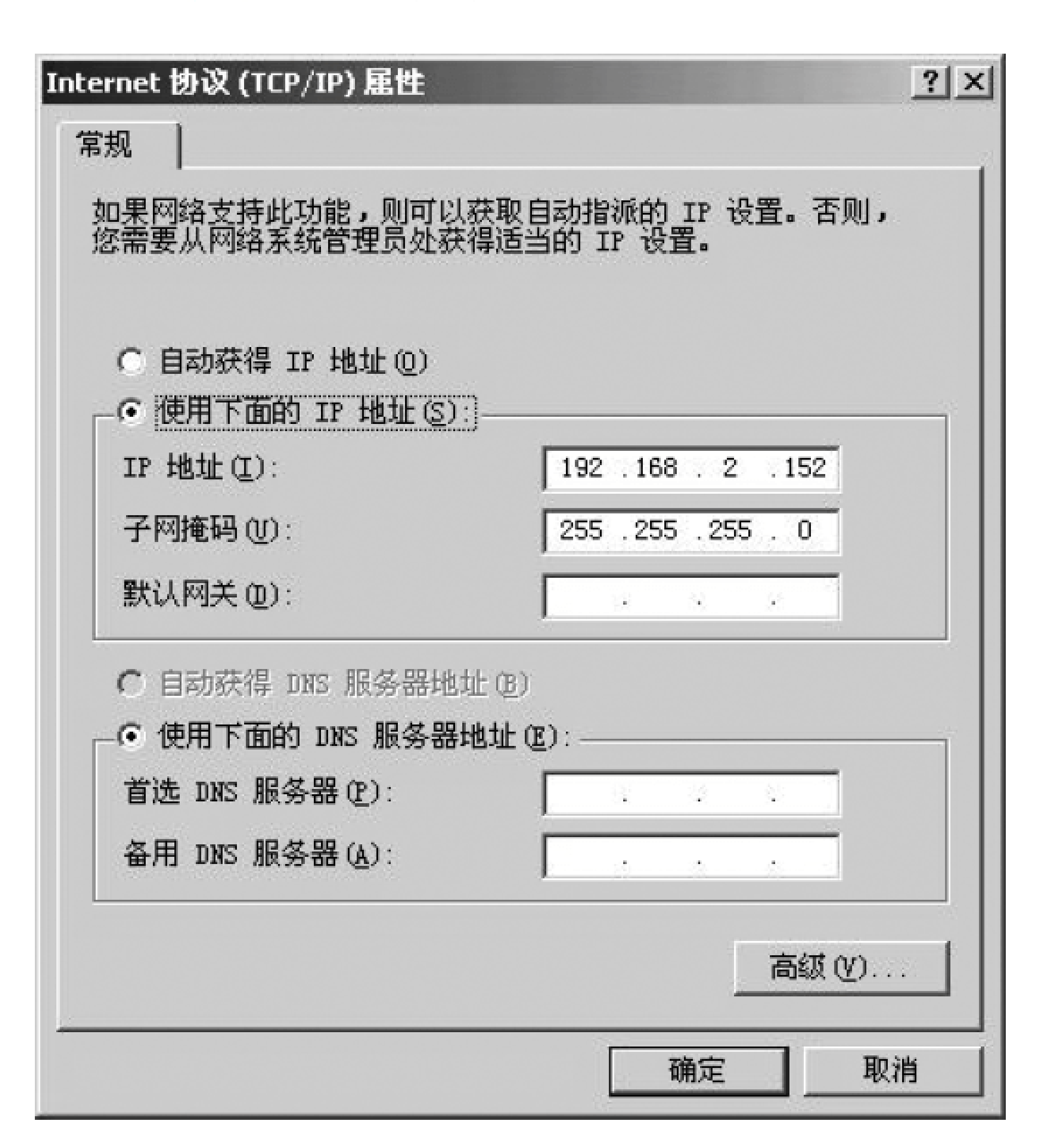


图 2-83　客户端 IP 设置

假如服务器端程序已在 192. 168. 2. 152 上运行了，通信方式为 TCP，端口为 54320。在另外一台计算机上解压 BO2K1. 1. 6，目录下的 bo2kgui. exe 就是 BO2K 的客户端系统。

（2）启动 bo2kgui. exe，如图 2-84 所示。



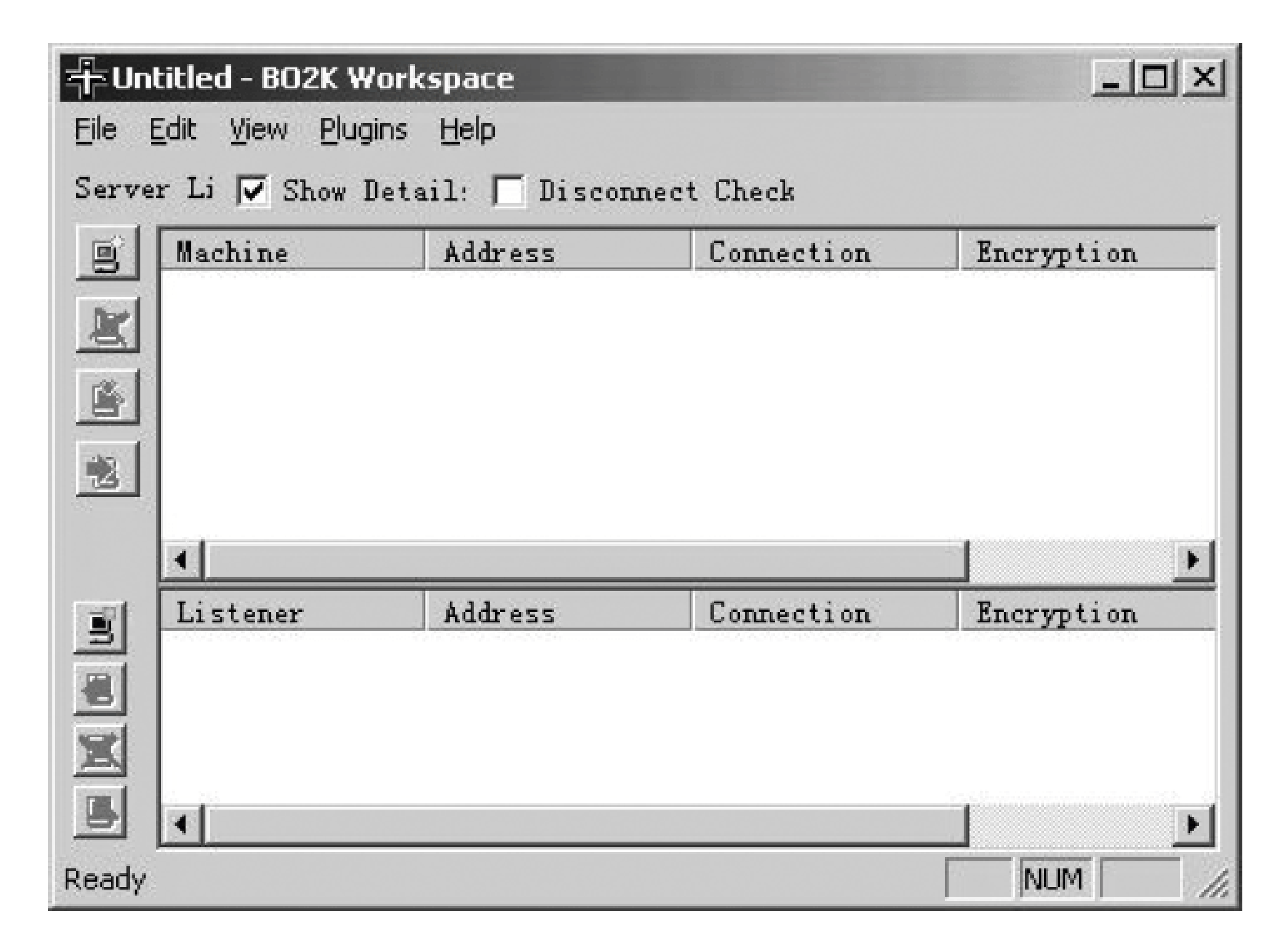


图 2-84　BO2K 客户端

(3) 插件配置。单击 Plugins(插件)/Configure(配置)命令,出现如图 2-85 所示的对话框,单击 Insert 按钮添加插件,插件在如图 2-78 所示的 plugins 文件夹中。添加的插件包括 auth、enc、io、misc、cli 目录下的所有 DLL 文件。可以通过 Option 列表框选择插件,并对插件进行配置。单击 Done(完成)按钮,关闭插件配置程序。

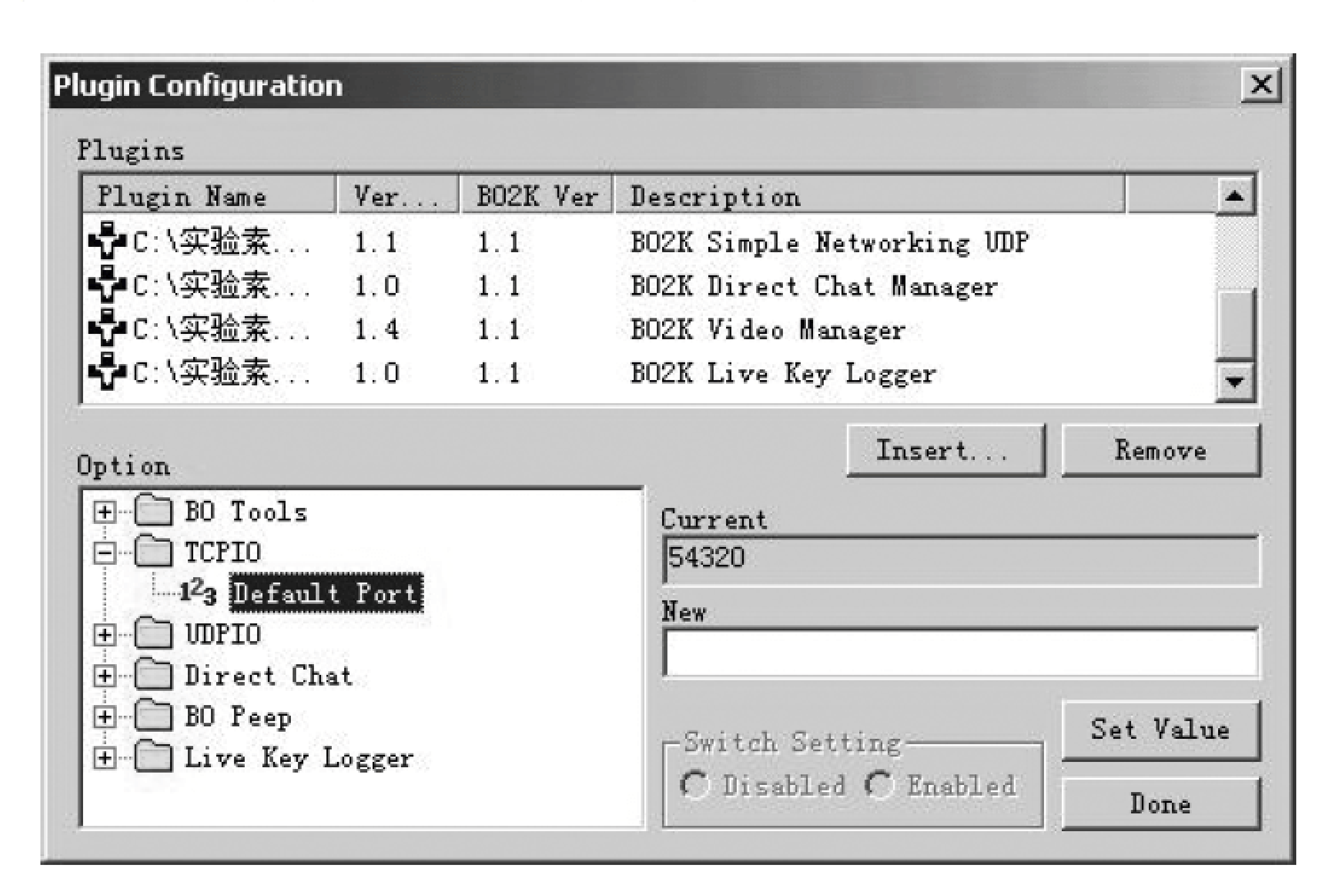


图 2-85　客户端插件配置

(4) 添加服务器。在客户端单击 File(文件)/New Server(新服务器)命令,添加一个服务器,如图 2-86 所示。输入服务器的地址和名称,在 Connection(连接)下拉列表框中选择合适的版本(例如选择 v1.0)。

(5) 启动连接。添加服务器成功,在客户端的服务器列表中将出现服务器信息,如图 2-87所示。

(6) 双击 thTest,出现连接界面,然后单击 Connect(连接)按钮,启动与服务器的连接,连接成功后出现如图 2-88 所示的控制台对话框。



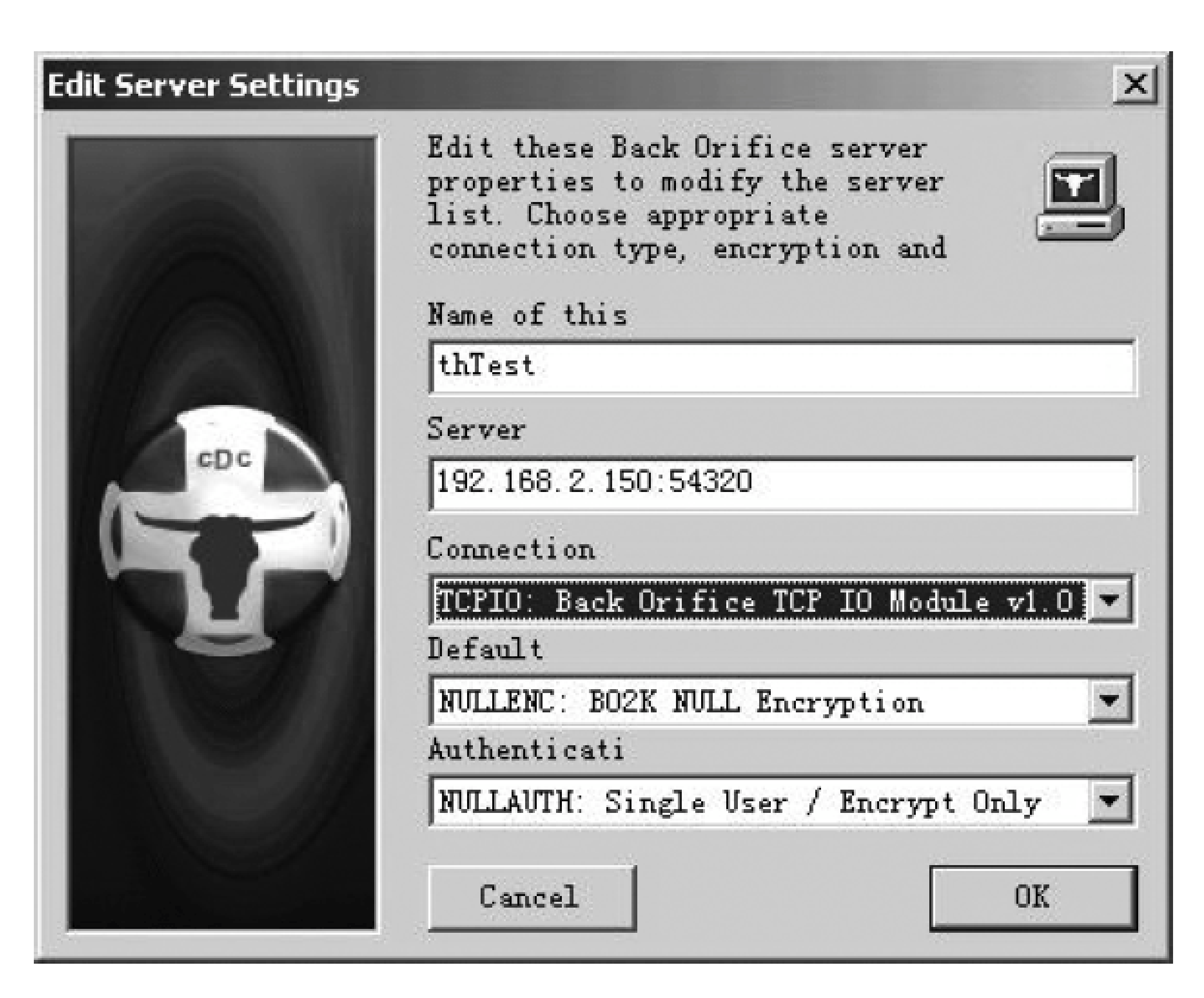


图 2-86　添加新服务器

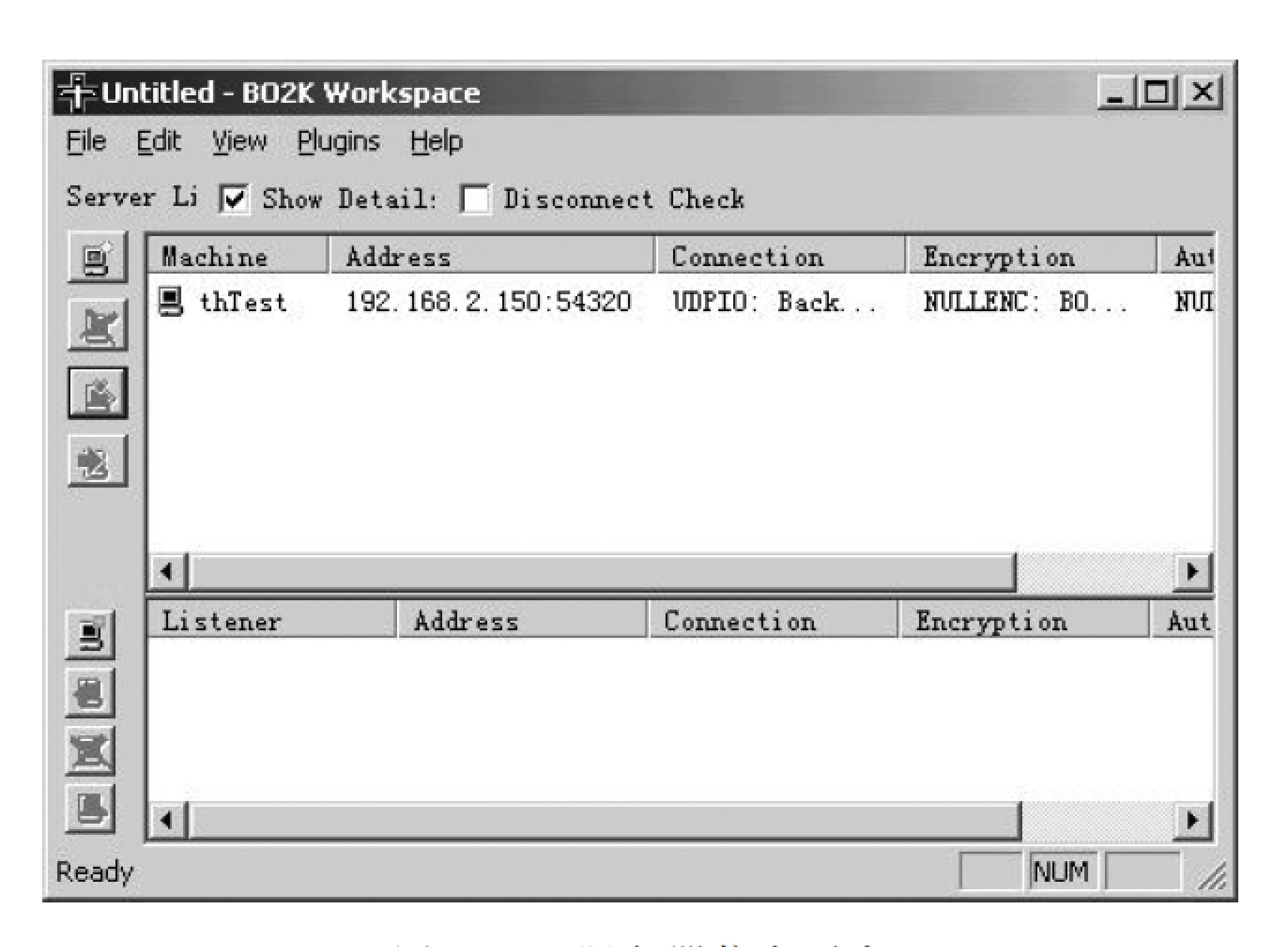


图 2-87　服务器信息列表

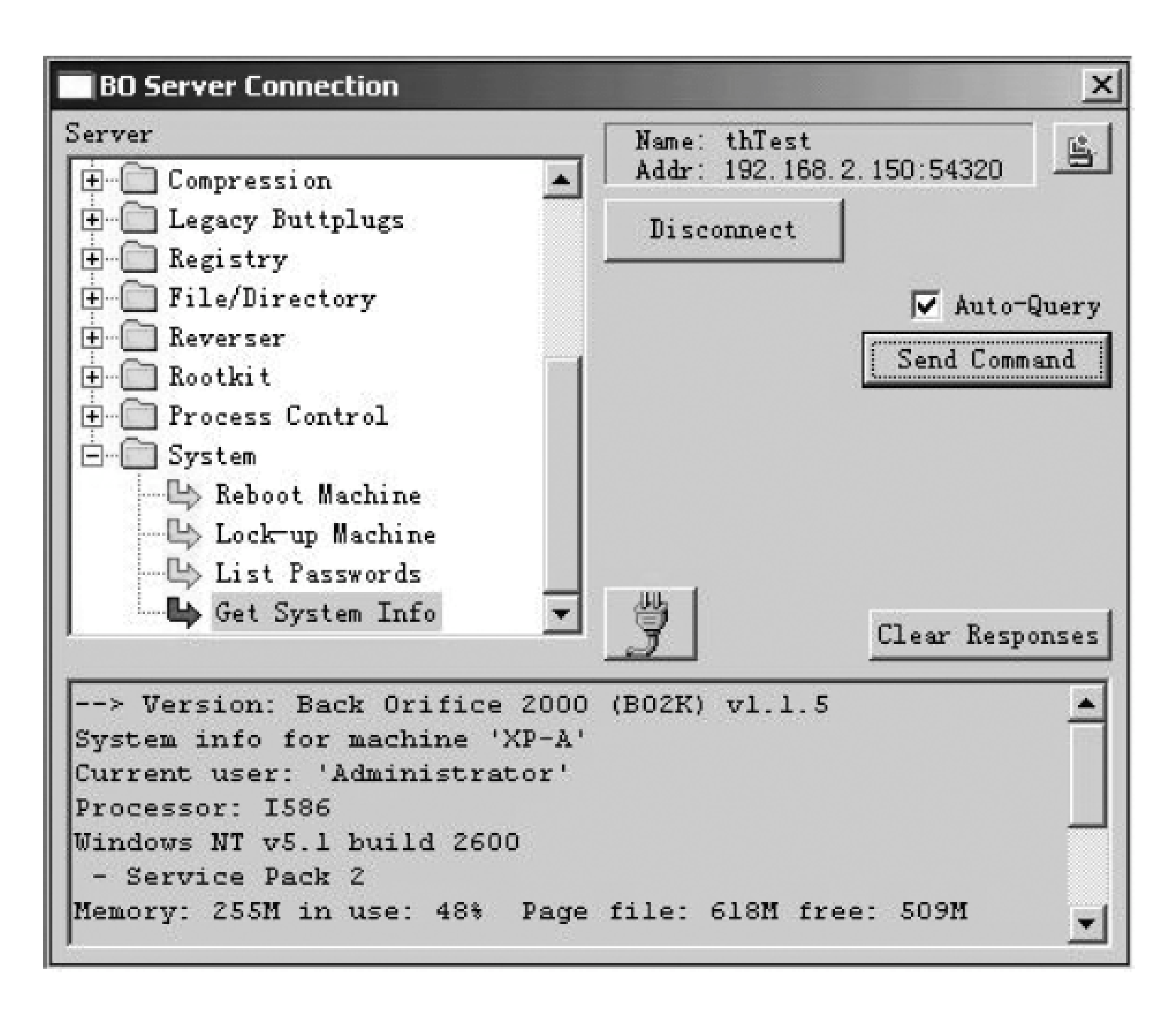


图 2-88　对远程服务器的控制



读者可参考 BO2K 的文档了解 BO2K 服务器的隐身技术并做测试;也可以尝试通过 BO2K 获取服务器上 E-mail、QQ 等软件的口令;最后可以尝试手工清除木马。

2.8 木马防范工具的使用

2.8.1 木马克星 2009 简介

木马克星(Iparmor)是一款适合网络用户的安全软件,既有面对新手的扫描内存和扫描硬盘功能,也有面对网络高手的众多调试查看系统功能。木马克星可以查杀 5021 种国际木马、112 种电子邮件木马,保证查杀冰河类文件关联木马、QQ 类寄生木马、ICMP 类幽灵木马、网络神偷类反弹木马。其内置木马防火墙,任何黑客试图与本机建立连接,都需要木马克星确认,不仅可以查杀木马,更可以查黑客。

木马克星 2009 是一款免费软件,无须注册即可以使用所有功能。

木马克星 2009 主要分两大部分的内容:功能和查看。其中“功能”部分(【功能】菜单,如图 2-89 所示)主要是针对一般用户的,其主要作用是扫描硬盘或内存中是否存在木马,并可以在此修改一些设置;“查看”部分(【查看】菜单,如图 2-90 所示)主要针对高级用户,主要作用是查看一些网络信息。下面对这两个部分的各个主要选项(命令)作简要介绍。



图 2-89 【功能】菜单

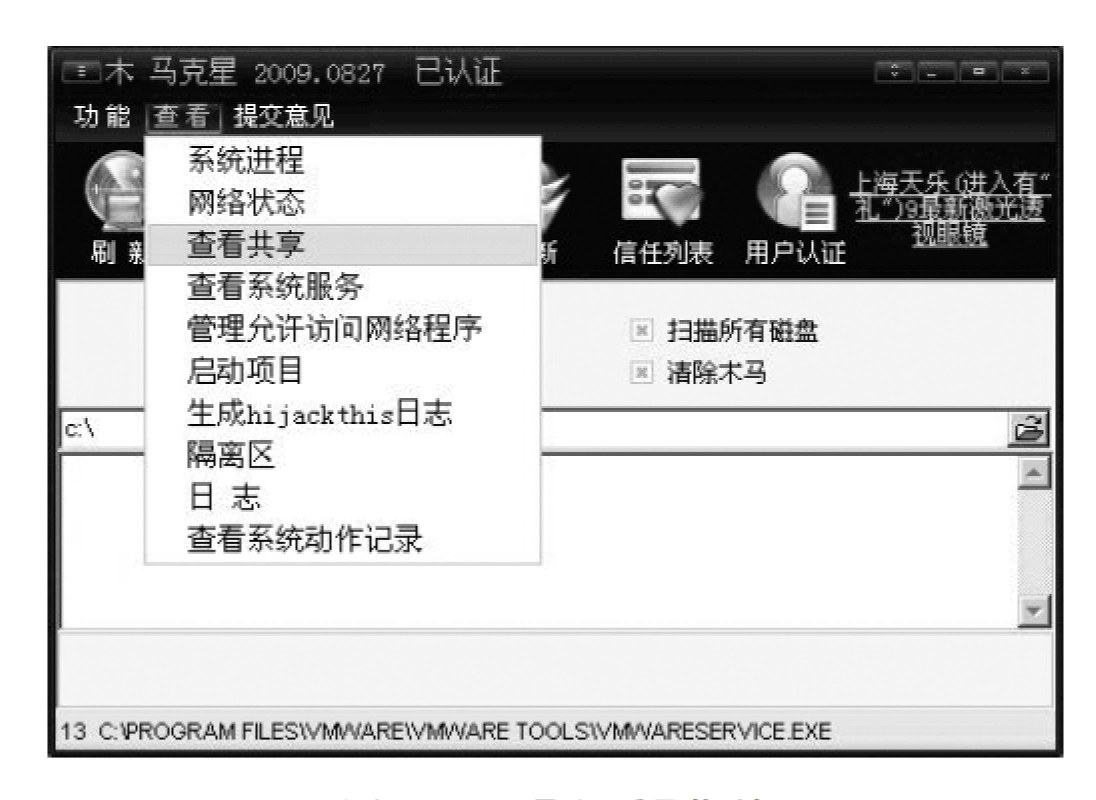


图 2-90 【查看】菜单

1. “功能”部分

(1) 扫描内存。软件启动后会自动进入此页面,它很直观地显示了当前内存中有没有木马,如果你是头 30 次使用,木马克星可以自动帮助你清除木马,不需要人工干预。当然,每日都有两三种新的木马病毒,为了更加安全,还是需要升级木马病毒库。

(2) 扫描硬盘。在此页面可以选择是否清除木马,在输入框的右边可以选择扫描路径,并可以进行全硬盘扫描。经常的扫描可以帮助用户清除硬盘中的木马。我们推荐每周至少扫描 1 次。

(3) 设置。可以选择软件是否在 Windows 启动的时候自动启动,这个防火墙主要针对蠕虫和端口监视,在用户接收 E-mail 时候,如果有蠕虫,它就会报警。当有黑客试图与用户计算机建立连接时,它也会报警。推荐使用此功能,扫描选项中用来设置硬盘扫描的文件类型,如果通过代理连接网络,还可以设置代理选项。



(4) 更新病毒库。建议用户每5天更新1次，如果更新时提示："已经是最新版本，不需要升级"，则代表已经用了最新版本，不需要升级。

(5) 刷新。单击后将会扫描内存，重新得到网络状态、系统进程、启动项目的信息。

2. "查看"部分

(1) 系统进程。在此页面可以看到系统中都有哪些程序在运行，用鼠标选择后，可以用键盘上的Delete键删除进程。

(2) 网络状态。在这里可以看到用户的网络情况，TCP协议的Listen如果在1025端口以上，则可能是木马。

(3) 查看共享。可以看到用户的硬盘是否在网络中公开。

(4) 启动项目。可以看到有哪些程序随Windows一起运行，用鼠标选择后，可以用键盘上的Delete键删除进程。

2.8.2　木马克星2009应用

1. 木马克星2009的下载与安装

(1) 从木马克星网站(http://www.luosoft.com)下载木马克星的最新版本。

(2) 双击来执行木马克星2009的安装文件tu2.exe，然后选择【我同意此协议】复选框，并单击【下一步】按钮。

(3) 根据需要选择文件安装目标位置(默认为C盘)，然后单击【下一步】按钮。

(4) 根据提示选择默认值，不断单击【下一步】按钮，然后单击【安装】按钮，程序会自动安装；最后，文件程序安装完毕，单击【完成】按钮即可。

2. 对木马克星2009工具进行配置

(1) 启动木马克星2009主程序。启动木马克星2009的主程序iparmor.exe，该程序在启动后首先会扫描内存页面，软件启动后进入如图2-91的界面，它很直观地显示了当前内存中有没有木马。

(2) 设置木马拦截选项。选择【功能】菜单中的【设置】命令，在打开的【设置】对话框中单击【木马拦截】标签，可以对木马拦截进行设置，如图2-92所示。



图2-91　木马克星2009程序界面



图2-92　设置木马拦截选项



- 网络拦截：就是网络防火墙，拦截一切非法程序。
- 监视网络信息：查看谁在连接本地主机的 IP 地址。
- 监视邮件：主要监视 POP3 类型的邮箱。
- 密码保护：主要是把用户的密码都伪装成 iparmor 这个词组，所有其他盗窃密码的软件所看到的都将是 iparmor。

(3) 设置扫描选项。在【设置】对话框的【扫描选项】选项卡中，可以对扫描选项进行设置，如图 2-93 所示。如果是第一次就选取扫描全部文件，第二次就可以按照图片上的项目有目的地进行选择。都选择好之后，单击【确认】按钮进行保存设置，否则选择【放弃】按钮。

3. 扫描木马病毒

单击工具栏上的【扫描硬盘】按钮，在打开的窗口中选中【扫描所有磁盘】和【清除木马】这两个复选框，如图 2-94 所示。单击【扫描】按钮，就开始对硬盘进行扫描并清除查找到的木马。



图 2-93　设置扫描选项



图 2-94　扫描硬盘

2.9　流氓软件

流氓软件是介于病毒和正规软件之间的软件。流氓软件同时具备正常功能(下载、媒体播放等)和恶意行为(弹广告、开后门)，会给用户带来实质性危害。这些软件也可能被称为恶意广告软件、间谍软件、恶意共享软件。与病毒或者蠕虫不同，这些软件很多不是小团体或者个人秘密地编写和散播，反而有很多知名企业和团体涉嫌此类软件，其中以雅虎旗下的 3721 最为知名和普遍，也比较典型。该软件采用多种技术手段强行安装和对抗删除。很多用户投诉是在不知情的情况下遭到安装，而其多种反卸载和自动恢复技术使得很多软件专业人员也感到难以对付，以至于其卸载方法成为网站上常常被讨论和咨询的技术问题。

2.9.1　流氓软件的主要特征

流氓软件是指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行侵害用户合法权益的软件，但不包含中国法律、法规规定的计算机病毒。





流氓软件的主要特征表现为以下几个方面。

(1) 强制安装：指未明确提示用户或未经用户许可，在用户计算机或其他终端上安装软件的行为。

(2) 难以卸载：指未提供通用的卸载方式，或在不受其他软件影响、人为破坏的情况下，卸载后仍然有活动程序的行为。

(3) 浏览器劫持：指未经用户许可，修改用户浏览器或其他相关设置，迫使用户访问特定网站或导致用户无法正常上网的行为。

(4) 广告弹出：指未明确提示用户或未经用户许可，利用安装在用户计算机或其他终端上的软件弹出广告的行为。

(5) 恶意收集用户信息：指未明确提示用户或未经用户许可，恶意收集用户信息的行为。

(6) 恶意卸载：指未明确提示用户、未经用户许可，或误导、欺骗用户卸载其他软件的行为。

(7) 恶意捆绑：指在软件中捆绑已被认定为恶意软件的行为。

(8) 其他行为：包括其他侵害用户软件安装、使用和卸载知情权、选择权的恶意行为。

2.9.2　流氓软件的分类

流氓软件主要包括：广告软件、浏览器劫持、行为记录软件、恶意共享软件、搜索引擎劫持软件、自动拨号程序、网络钓鱼和垃圾邮件等。

(1) 广告软件(Adware)：广告软件指未经用户允许，下载并安装在用户计算机上；或与其他软件捆绑，通过弹出式广告等形式谋取商业利益的程序。

(2) 浏览器劫持(Brower Hijack)：浏览器劫持是一种恶意程序，通过浏览器插件、BHO(浏览器辅助对象)、Winsock LSP 等形式对用户的浏览器进行篡改，使用户的浏览器配置不正常，或被强行引导到商业网站。

(3) 行为记录软件(Track Ware)：行为记录软件指未经用户许可，窃取并分析用户隐私数据，记录用户计算机使用习惯、网络浏览习惯等个人行为的软件。

(4) 恶意共享软件(Malicious Shareware)：恶意共享软件指采用不正当的捆绑或不透明的方式强制安装在用户的计算机上，并且利用一些病毒常用的技术手段造成软件很难被卸载，或采用一些非法手段强制用户购买免费、共享软件。

(5) 搜索引擎劫持软件：搜索引擎劫持是指未经用户授权，自动修改第三方搜索引擎结果的软件。

(6) 自动拨号程序(Dialer)：自动拨号程序指自动下载并安装到用户的计算机上，并隐藏在后台运行。它会自动拨打长途或收费电话，以赚取用户高额的电话费用。

(7) 网络钓鱼(Phishing)：网络钓鱼一词，是“Phone”和“Fishing”的综合体。由于黑客始祖起初是以电话作案，所以用“Ph”来取代“F”，创造了“Phishing”。Phishing 发音与 Fishing 相同。网络钓鱼是指攻击者利用欺骗性的电子邮件和伪造的 Web 站点来进行网络诈骗活动，受骗者往往会泄露自己的私人资料，如信用卡号、银行卡账户、身份证号等内容。诈骗者通常会



将自己伪装成网络银行、在线零售商和信用卡公司等可信的品牌，骗取用户的私人信息。

(8) 垃圾邮件(Spam)：垃圾邮件也是非常熟悉和讨厌的一种恶意软件，平常所收到的邮件中至少有一半以上的邮件都是不请自来的垃圾邮件。这些垃圾邮件中，有的是商业广告，有的则带有病毒文件和图片，还有些是不健康的交友宣传等。

2.9.3 流氓软件的防范

防止流氓软件入侵的方法主要有以下几个方面：

(1) 养成良好健康的上网习惯，不访问不良网站，不随便点击小广告。

(2) 下载要安装的软件尽量到该软件的官方网站，或者到信任度高的下载站点进行下载。

(3) 安装软件的时候，每个安装步骤最好能仔细看清楚，防止捆绑软件入侵。

(4) 安装如 360 安全卫士等安全类软件，定时对系统做诊断，查杀流氓软件，如图 2-95 所示。



图 2-95 用 360 安全卫士查杀流氓软件

2.10 习 题

1. 简述计算机病毒的主要特点。
2. 简述计算机病毒有哪几种分类。
3. 简述不同类型病毒的特征和危害。
4. 简述计算机病毒的发展趋势。
5. 简述部署企业网络防病毒系统的步骤。
6. 比较蠕虫病毒与计算机病毒，它们的区别在哪里？



7. 蠕虫病毒的预防措施主要有哪些？
8. 简述狙击波蠕虫的预防方法和步骤。
9. 简述木马的组成。木马软件部分主要由什么组成？
10. 木马有哪些危害？
11. 识别和清除木马的方法有哪些？
12. 如何防范流氓软件？



第3章 黑客攻击及其防御

本章学习目标

- 掌握黑客攻击的方法、步骤和原理。
- 掌握拒绝服务攻击的原理、应用与防御方法。

网络就像一个潘多拉魔盒，光怪陆离、无所不有。网络在给人们的生活带来无穷乐趣的同时，在一般人不留意的网络深处，还存在着一群神秘的群体——黑客！是他们使网络充斥着太多的骗局和陷阱，不时地令冲浪者防不胜防，这个无法回避的事实告诫人们：在网上要时刻保持足够的警惕，那么应如何做呢？

3.1 认识黑客及其攻击手段

3.1.1 黑客与黑客攻击

黑客(Hacker)是一群对计算机有着强烈好奇心且技术高超的计算机精英，他们具有操作系统和编程方面的高级知识，知道系统中的漏洞及其原因所在；他们是非法的入侵者。

黑客攻击其实质就是指利用被攻击方信息系统自身存在的安全漏洞，通过使用网络命令和专用软件进入对方网络系统的攻击。

3.1.2 黑客攻击的手段

目前黑客网络攻击的类型主要有以下几种：

(1) 利用监听嗅探技术获取对方网络上传输的有用信息。

(2) 利用拒绝服务攻击，使目的网络暂时或永久性瘫痪。

(3) 利用网络协议上存在的漏洞进行网络攻击。

(4) 利用系统漏洞，例如缓冲区溢出或格式化字符串等，以获得目的主机的控制权。

(5) 利用网络数据库存在的安全漏洞，获取或破坏对方的重要数据。

(6) 利用计算机病毒传播快、破坏范围广的特性，开发合适的病毒破坏对方网络。

以上类型所采用的攻击手法主要有如下几种。



1. 网络监听

最初,网络嗅探是应用于网络管理,就像远程控制软件一样,但后来这些强大的功能逐渐被黑客们利用。最普遍的安全威胁来自内部,同时这些威胁通常都是致命的,其破坏性也远大于外部威胁。对于安全防护一般的网络,使用网络嗅探这种方法操作简单,而且同时威胁巨大。很多黑客也使用嗅探器进行网络入侵的渗透。网络嗅探器对信息安全的威胁来自其被动性和非干扰性,使得网络嗅探具有很强的隐蔽性,往往让网络信息泄密变得不容易被发现。

对于网络嗅探攻击,可以采取以下一些措施来应对。

(1) 网络分段:一个网络段包括一组共享低层设备和线路的机器,如交换机、动态集线器和网桥等设备,可以对数据流进行限制,从而达到防止嗅探的目的。

(2) 加密:一方面可以对数据流中的部分重要信息进行加密;另一方面也可只对应用层加密,然而后者将使大部分与网络和操作系统有关的敏感信息失去保护。选择何种加密方式就取决于信息的安全级别及网络的安全程度。

(3) 一次性口令技术:口令并不在网络上传输,而是在两端进行字符串匹配,客户端利用从服务器上得到的 Challenge 和自身的口令计算出一个新字符串,并将之返回给服务器。在服务器上利用比较算法进行匹配,如果匹配连接就允许建立,所有的 Challenge 和字符串都只使用一次。

(4) 禁用混杂节点:安装不支持混杂模式的网卡,通常可以防止 IBM 兼容机进行嗅探。

2. 拒绝服务攻击

拒绝服务攻击是目前最常见的一种攻击类型。从网络攻击的各种方法和所产生的破坏情况来看,DoS(Denial of Service,拒绝服务)算是一种很简单但又很有效的进攻方式,它的目的就是拒绝服务访问,破坏组织的正常运行,最终使网络连接堵塞,或者服务器因疲于处理攻击者发送的数据包而使服务器系统的相关服务崩溃、系统资源耗尽,其原理如图 3-7 所示。

DoS 攻击方式有很多,最基本的就是利用合理的服务请求来占用过多的服务资源,从而使合法用户无法得到服务。DoS 攻击的基本过程如下:首先攻击者向服务器发送众多的带有虚假地址的请求,服务器发送回复信息后等待回传信息。由于地址是伪造的,所以服务器一直等不到回传的消息,然而服务器中分配给这次请求的资源就始终没有被释放。当服务器等待一定的时间后,连接会因超时而被切断,攻击者会再度传送新的一批请求,在这种反复发送伪地址请求的情况下,服务器资源最终会被耗尽。

DDoS(Distributed Denial of Service,分布式拒绝服务)是一种基于 DoS 的特殊形式的分布、协作式的大规模拒绝服务攻击。也就是说不再是单一的服务攻击,而是同时实施几个甚至十几个不同服务的拒绝攻击。由此可见,它的攻击力度更大,危害性当然也更大了。它主要瞄准比较大的网站,像商业公司、搜索引擎和政府部门的 Web 站点。

防火墙和 VPN(Virtual Private Network,虚拟专用网)是目前阻挡 DoS 攻击的常用设备。其中,防火墙作为访问控制设备,通过设计访问策略,能够对 DoS 攻击起到一定防范作



用。不过，当防火墙依据多重安全规则，对不同服务进行数据包过滤和代理时，容易导致系统管理者将防火墙的环境设定错误，而留下一些系统安全漏洞，让入侵者有机可乘。

3. 源 IP 地址欺骗

许多应用程序认为如果数据包能够使其自身沿着路由到达目的地，而且应答包也可以回到源地，那么源 IP 地址一定是有效的，而这正是使源 IP 地址欺骗攻击成为可能的前提。

要防止源 IP 地址欺骗行为，可以采取以下措施来尽可能地保护系统免受攻击。

(1) 抛弃基于地址的信任策略：阻止这类攻击的一种非常容易的办法就是放弃以地址为基础的验证。不允许 r 类远程调用命令删除. rhosts 文件，清空/etc/hosts 下的 equiv 文件。这将迫使所有用户使用其他远程通信手段，如 Telnet、ssh 和 skey 等。

(2) 使用加密方法：在包发送到网络上之前，可以对它进行加密。虽然加密过程要求适当改变目前的网络环境，但它将保证数据的完整性和真实性。

(3) 进行包过滤：可以配置路由器使其能够拒绝网络外部与本网内具有相同 IP 地址的连接请求。而且，当包的 IP 地址不在本网内时，路由器不应该把本网主机的包发送出去。

注意：路由器虽然可以封锁试图到达内部网络的特定类型的包，但它们也是通过分析测试源地址来实现操作的，因此，它们仅能对声称是来自于内部网络的外来包进行过滤。若你的网络存在外部可信任主机，那么路由器将无法防止别人冒充这些主机进行 IP 欺骗。

4. 源路由欺骗攻击

在通常情况下，信息包从起点到终点走过的路径是由位于此两点间的路由器决定的，数据包本身只知道去往何处，但不知道该如何去。源路由可使信息包的发送者将此数据包要经过的路径写在数据包里，使数据包循着一个对方不可预料的路径到达目的主机。

对付这种攻击最好的办法是配置好路由器，使它抛弃那些由外部网进来的却声称是内部主机的报文。

5. 缓冲区溢出

为了便于理解，我们不妨打个比方。缓冲区溢出好比是将 10 磅的糖放进一个只能装 5 磅的容器里。一旦该容器放满了，余下的部分就溢出在柜台和地板上，弄得一团糟。由于计算机程序的编写者写了一些编码，但是这些编码没有对目的区域或缓冲区，即 5 磅的容器做适当的检查，看它们是否够大，能否完全装入新的内容——10 磅的糖，结果可能造成缓冲区溢出的产生。如果打算放进新地方的数据不适合，到处溢出，该数据也会制造很多麻烦。但是，如果缓冲区仅仅溢出，这只是一个问题。到此时为止，它还没有破坏性。当糖溢出时，柜台被盖住。可以把糖擦掉或用吸尘器吸走，还柜台本来面貌。与之相对的是，当缓冲区溢出时，过剩的信息覆盖的是计算机内存中以前的内容。除非这些被覆盖的内容被保存或能够恢复，否则就会永远丢失。

缓冲区溢出是病毒编写者和特洛伊木马编写者偏爱使用的一种攻击方法。攻击者或者病毒善于在系统当中发现容易产生缓冲区溢出之处，以运行特别程序，并获得优先级，指示



计算机破坏文件，改变数据，泄露敏感信息，产生后门访问点，感染或者攻击其他计算机。

webdavx3.exe 是针对 Windows 2000 中文版的溢出工具，不用 NC 监听端口，溢出成功后直接用 Telnet ip 7788 操作即可。

防范措施如下：设置复杂的开机密码；关闭 Telnet 服务。

6. 密码攻击

密码攻击通过多种不同方法实现，包括蛮力攻击(brute force attack)、特洛伊木马程序、IP 欺骗和报文嗅探。尽管报文嗅探和 IP 欺骗可以捕获用户账号和密码，但密码攻击通常指的是反复地试探、验证用户账号或密码，这种反复试探被称为蛮力攻击。

其防范措施如下：

(1) 使用有效安全的密码。主要包括密码应当遵循字母、数字、大小写混合使用的规则。

(2) 使用如＃或％或＄这样的特殊字符也能增加密码的复杂性。

7. 应用层攻击

应用层攻击能够使用多种不同的方法来实现，最常见的方法是使用服务器上通常可找到的应用软件(如 SQL Server、Sendmail、PostScript 和 FTP)缺陷，通过使用这些缺陷，攻击者能够获得计算机的访问权，以及在该计算机上运行相应应用程序所需账户的许可权。

在应用层攻击中，容易遭受攻击的目标包括路由器、数据库、Web 和 FTP 服务器及与协议相关的服务，如 DNS、WINS 和 SMB。

防范方法如下：

(1) 避免下载可疑程序并拒绝执行，运用网络扫描软件定期监视内部主机并监听 TCP 服务。

(2) 通过数据加密和身份认证(如智能卡、一次性口令等)来保护数字资产，防止未经授权泄露重要电子信息。

3.2　黑客攻击的基本步骤

黑客攻击的基本步骤可以用图 3-1 来表示。

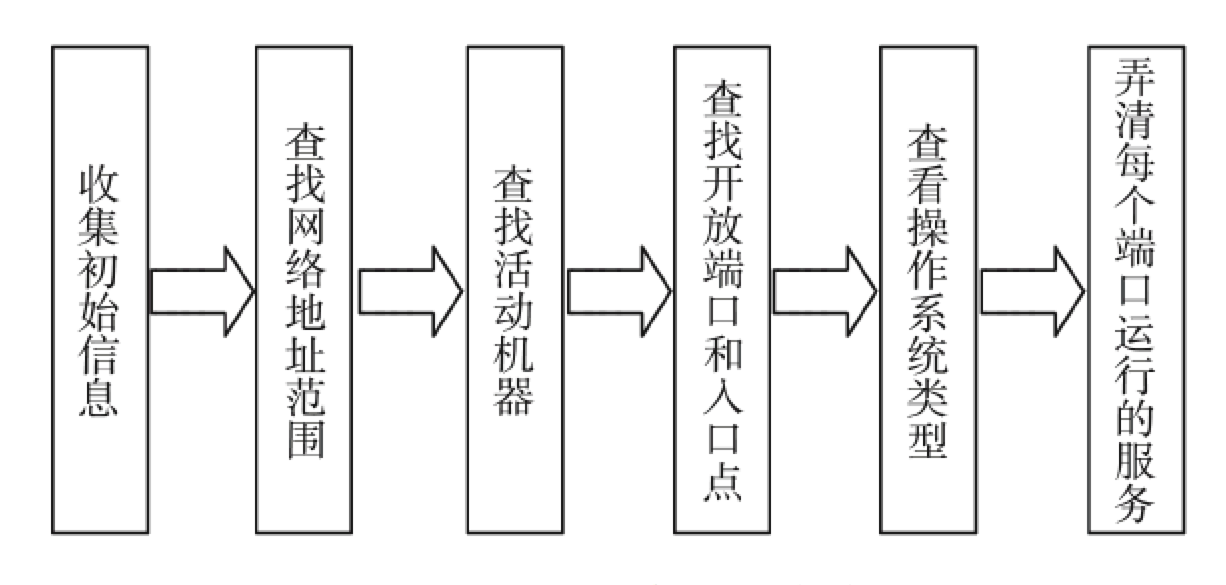


图 3-1　黑客攻击的基本步骤



3.2.1 收集初始信息

黑客们总是希望知道尽可能多的信息，比如，是否联网、内部网络的架构以及安全防范措施的状态。

收集初始信息可先获取 IP 地址。获取 IP 地址的简单方法是用 ping 命令，设法把主机名解析为 IP 地址并输出到屏幕。例如使用 ping hao123.com 命令，可以得到 hao123 网址之家网站的 IP 地址。但如果网络不顺畅，将会出现如图 3-2 所示的结果。处理方法是查看网络连接状态，重新用 ping 命令。当攻击者得到网络的 IP 地址，能够把此网络当作初始攻击点。

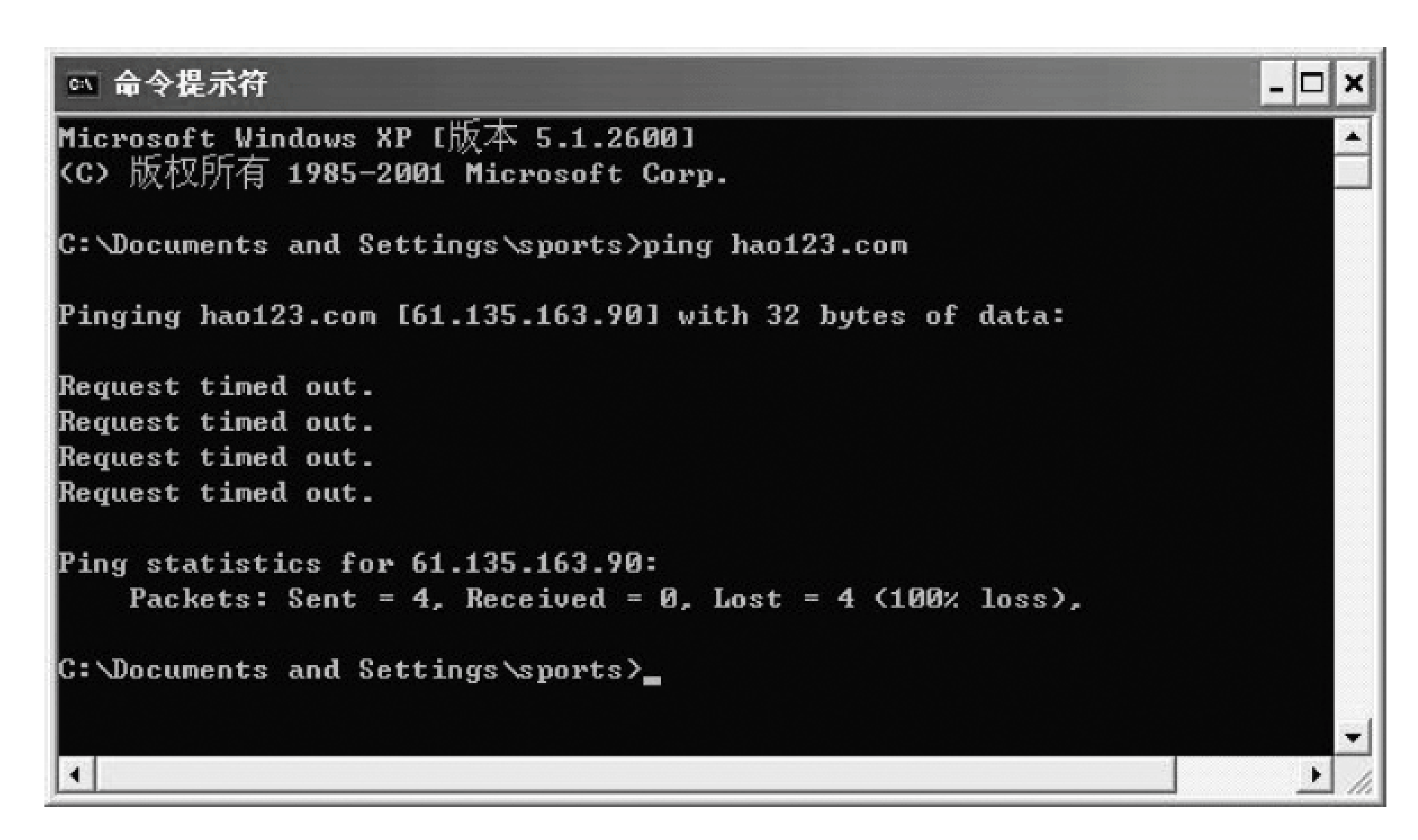


图 3-2 Ping hao123 网址之家的结果显示

3.2.2 查找网络地址范围

当攻击者有一些机器的 IP 地址后，下一步就需要找出网络的地址范围或者子网掩码，以保证能集中精力对付一个网络而没有闯入其他网络。这样做有两个原因：第一，假设有地址 10.50.60.7，要扫描整个 A 类地址需要一段时间，如果正在跟踪的目标只是地址的一个小子集，那么就无须浪费时间；第二，一些公司有比其他公司更好的安全性，因此跟踪较大的地址空间增加了危险。

在 Internet 上，信息的传送是通过网中许多段的传输介质和设备(路由器、交换机、服务器、网关等)从一端到达另一端。每一个连接在 Internet 上的设备，如主机、路由器、接入服务器等，一般情况下都会有一个独立的 IP 地址。通过 tracert 命令可以知道信息从当前计算机到互联网另一端的主机走的是什么路径。

连接到 Internet 上的公司有一个外部服务器把网络连到 ISP 或者 Internet 上，所有去公司的流量必须通过外部路由器，否则没有办法进入网络。并且大多数公司有防火墙，所以 tracert 输出的最后一跳会是目的机器，倒数第二跳会是防火墙，倒数第三跳会是外部路由器。通过相同外部路由器的所有机器属于同一网络，通常也属于同一公司。因此

攻击者查看通过 tracert 到达的各种 IP 地址，看这些机器是否通过相同的外部路由器，就知道它们是否属于同一网络。例如使用 tracert 命令可以查看某台计算机到达网易网站的路由点，如图 3-3 所示。

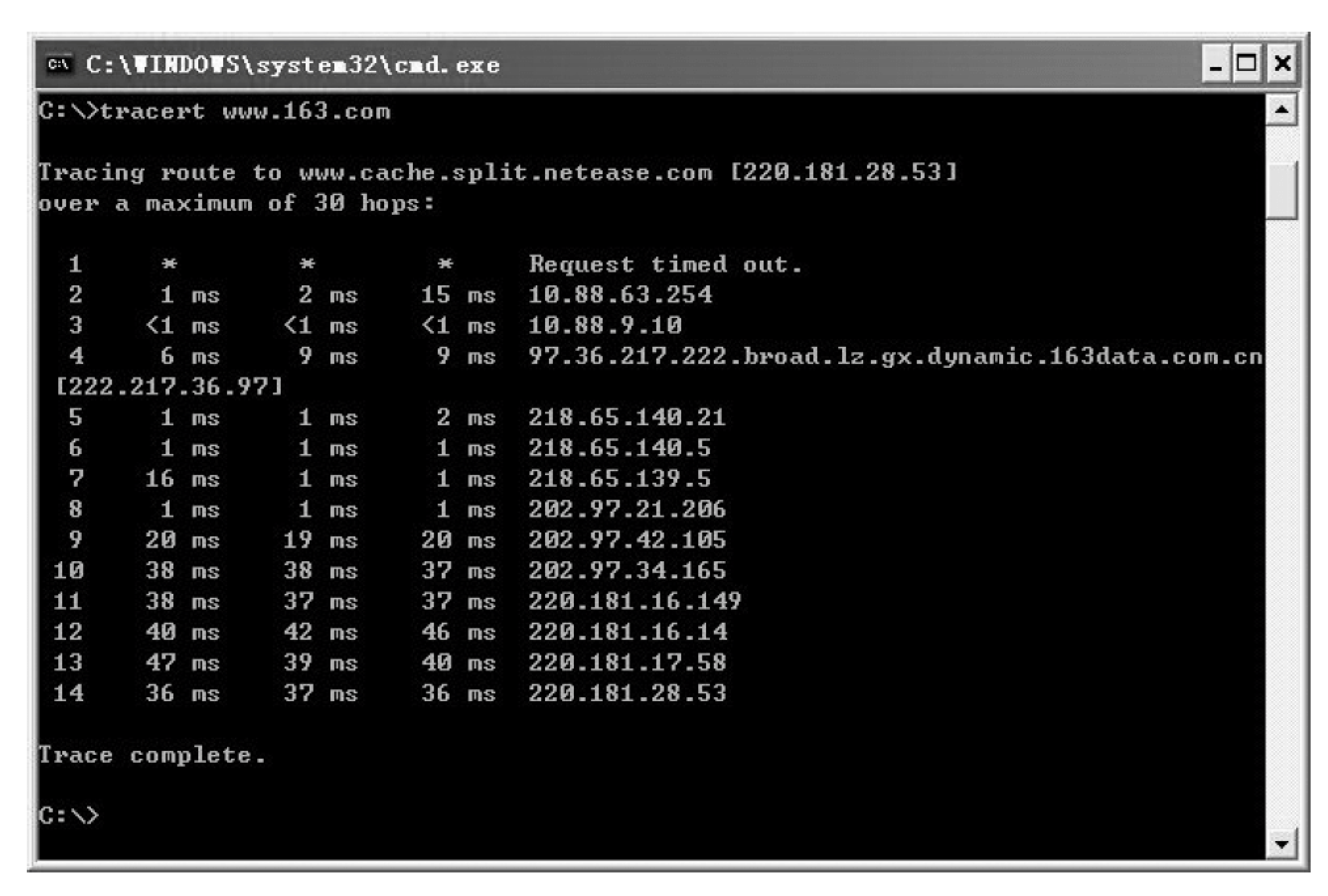


图 3-3　使用 tracert 命令的结果

3.2.3　查找活动机器

在知道了 IP 地址范围后，攻击者会想知道哪些机器是活动的，哪些不是。公司里一天中不同的时间有不同的机器在活动。一般攻击者在白天寻找活动的机器，然后在深夜再次查找，他就能区分工作站和服务器，因为服务器会一直被使用，而工作站只在正常工作日是活动的。

使用 ping 可以找到网络上哪些机器是活动的。但 ping 有一个缺点，一次只能 ping 一台机器。攻击者希望同时 ping 多台机器，看哪些有反应，这种技术一般被称为 Ping Sweeping。可以使用 Ping War 程序。图 3-4 所示是使用 Ping War 程序查找活动机器。查找结果与网络是否畅通有关，不同的网站因防范措施不同，会有不同的显示结果。Nmap 软件也能用来确定哪些机器是活动的。

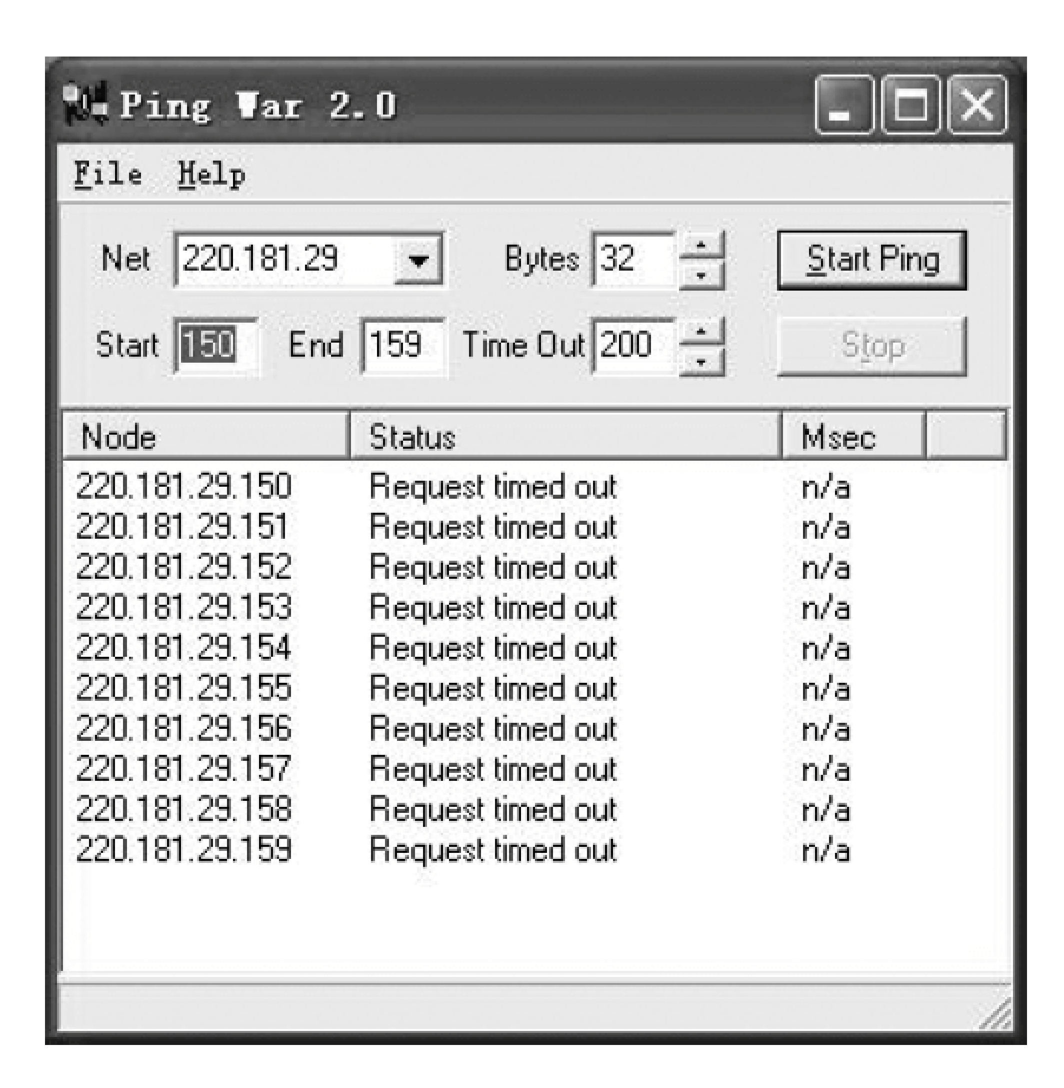


图 3-4　用 Ping War 查找活动机器



3.2.4 查找开放端口和入口点

网络通信除了需要知道目标 IP 地址外，还需要知道对方开放的端口。所以黑客攻击前也要知道可以利用的端口，此时可以利用 Port Scanners（端口扫描器）工具软件进行。端口扫描器在一系列端口上运行可以找出哪些是开放的。

选择端口扫描仪的两个关键特征：首先它能一次扫描一个地址范围；其次它能设定程序扫描的端口范围（能扫描 1～65 535 的整个范围）。

可以使用 nmap 的命令方式，目前流行的扫描类型：TCP connect 扫描、TCP SYN 扫描、FIN 扫描、ACK 扫描。图 3-5 所示是 TCP SYN 的扫描结果。



图 3-5　TCP SYN 扫描结果

3.2.5 查看操作系统类型

可以使用 nmap 中的-O 选项激活对 TCP/IP 指纹特征（fingerprinting）的扫描，获得远程主机的标志。即 nmap 使用一些技术检测目标主机操作系统网络协议栈的特征，把它和已知的操作系统指纹特征数据库做比较，就可以知道目标主机操作系统的类型。如图 3-6 所示是用 nmap 查看 IP 地址为 192.168.6.170 的远程主机的操作系统。

3.2.6 弄清每个端口运行的服务

弄清楚每个端口运行的服务可以有多种方法，简要介绍如下：

（1）default port and OS 是基于公有的配置和软件，攻击者能够比较准确地判断出每个







图 3-6 查看操作系统类型

端口在运行什么服务。例如如果知道操作系统是 UNIX 和端口 25 是开放的，就能判断出机器正在运行 sendmail；如果操作系统是 Microsoft NT 和端口 25 是开放的，就能判断出正在运行 Exchange。

(2) Telnet 是安装在大多数操作系统中的一个程序，它能连接到目的机器的特定端口上。攻击者使用这类程序连接到开放的端口上，大多数操作系统的默认安装显示了关于给定的端口在运行何种服务的标题信息。

(3) Vulnerability Scanners(弱点扫描器)是能被运行来对付一个站点的程序，它向黑客提供一张目标主机弱点的清单。

(4) 通过 TCP SYN 扫描就可以弄清楚每个端口运行的服务，如图 3-7 所示。

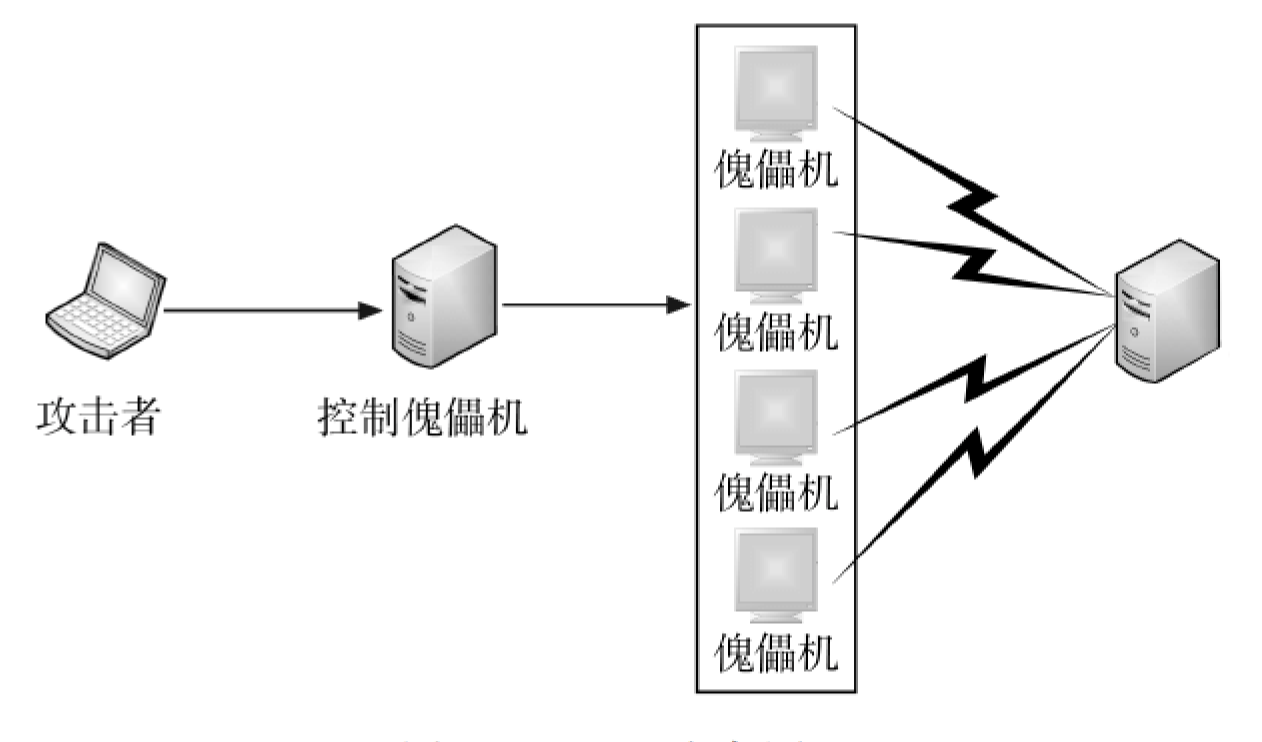


图 3-7 DoS 攻击原理



要保护网络免遭 SYN 攻击，只需按以下这些通用步骤操作即可：

(1) 启用 SYN 攻击保护。

(2) 设置 SYN 保护阈值。

(3) 设置其他保护。

经过一系列的前期准备，攻击者搜集了很多信息，确切地知道哪些机器是活动的，哪些不是，每一台机器正在使用的操作系统、开放的端口和运行的服务等信息。可以想象一下，他成功地攻击网络还困难吗？回答是否定的。当拥有了那些信息后，网络实际上相当于受到了攻击。因此，设法让攻击者不能获得太多的网络信息是关键。

3.3 拒绝服务攻击与防范

Sniffer（嗅探器）是一种威胁性极大的被动攻击工具。使用这种工具，可以监视网络的状态、数据流动情况以及网络上传输的信息。当信息以明文的形式在网络上传输时，便可以使用网络监听的方式来进行攻击。将网络接口设置在监听模式，便可以将网上传输的源源不断的信息截获。

Sniffer Pro 可运行在局域网的任何一台机器上，如果是练习使用，网络连接最好用 Hub 且在一个子网中，这样能抓到连到 Hub 上每台机器传输的包。

3.3.1 使用 Sniffer 软件监视网络的状态

使用 Sniffer 软件监视网络状态的步骤如下：

(1) 在被攻击计算机 B 中打开 Sniffer Pro 4.7.5，选择 Monitor/Matrix 命令，此时可看到网络中的 Traffic Map 视图，从任意主机发送给计算机 B 的 IP 数据包，如图 3-8 所示。

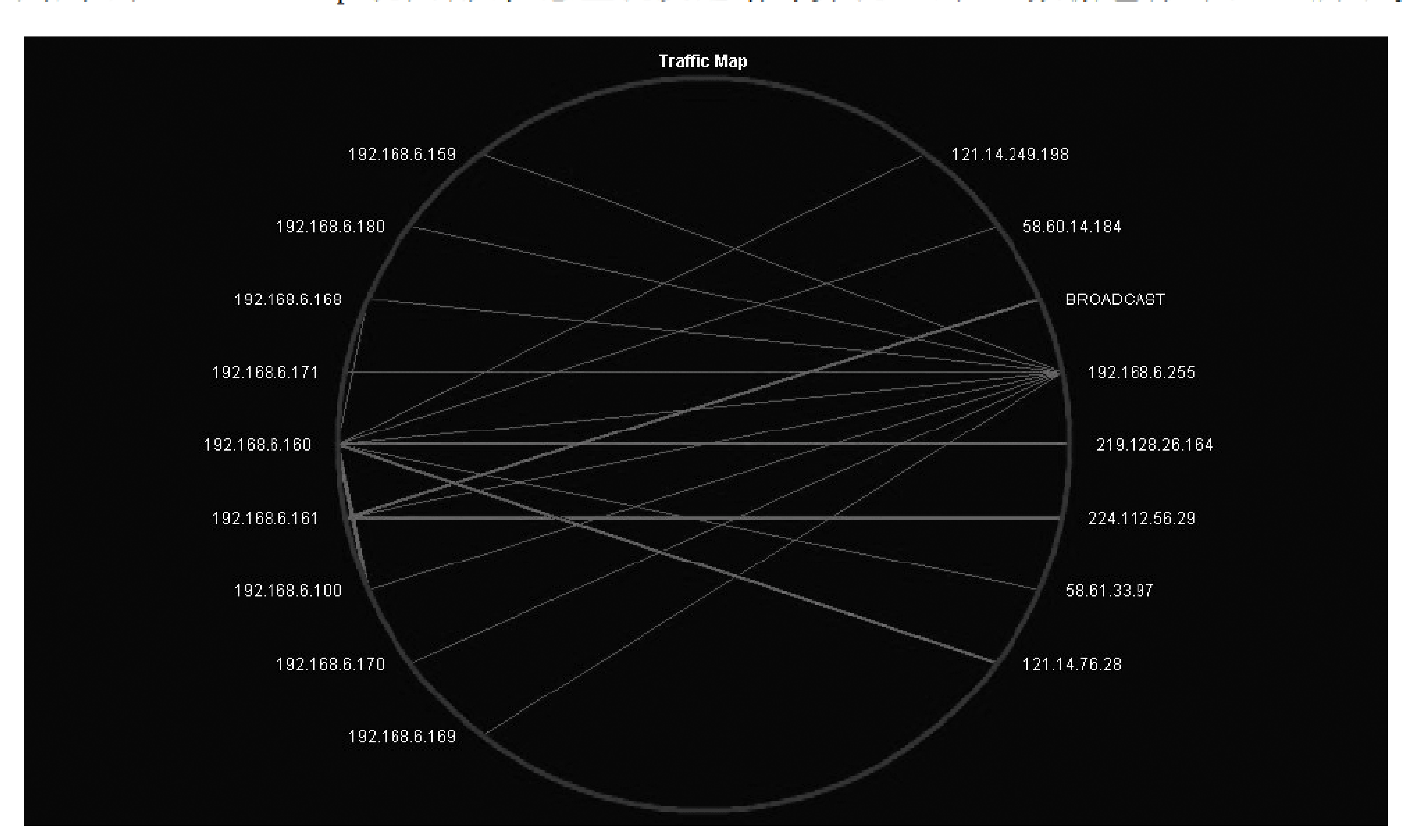


图 3-8 查看 Traffic Map 视图

(2) 打开进行攻击的计算机 A,将 XDOS 的可执行文件 xdos.exe 复制到 C 盘的根目录,打开命令行提示窗口,运行 cmd 命令,再运行 C:\xdos 命令,如图 3-9 所示。

```
C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>cd\

C:\>xdos
X-DOS v1.0 - command line d.o.s tool
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxx

Usage: xdos <Host> <Ports Scope> [Options]
<Ports Scope> means:
  <Start Port>[-<End Port>][,Port1,Port2-Port3,...]
[Options] means:
  -t <count>: specify threads count, default is 10
  -s <ip>   : specify source ip address ("*" means random ip)

Example: xdos www.xxx.com 80
         xdos 192.168.1.1 80,139 -t 5 -s *

C:\>_
```

图 3-9 运行 C:\xdos 命令

(3) 运行 xdos.exe,如图 3-10 所示。

```
C:\WINNT\system32\cmd.exe
<Ports Scope> means:
  <Start Port>[-<End Port>][,Port1,Port2-Port3,...]
[Options] means:
  -t <count>: specify threads count, default is 10
  -s <ip>   : specify source ip address ("*" means random ip)

Example: xdos www.xxx.com 80
         xdos 192.168.1.1 80,139 -t 5 -s *

C:\>xdos.exe
X-DOS v1.0 - command line d.o.s tool
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxx

Usage: xdos <Host> <Ports Scope> [Options]
<Ports Scope> means:
  <Start Port>[-<End Port>][,Port1,Port2-Port3,...]
[Options] means:
  -t <count>: specify threads count, default is 10
  -s <ip>   : specify source ip address ("*" means random ip)

Example: xdos www.xxx.com 80
         xdos 192.168.1.1 80,139 -t 5 -s *

C:\>
```

图 3-10 运行 xdos.exe

(4) 输入命令:xdos 192.168.6.160 80-t 200-s * ,确定即可进行攻击,如图 3-11 所示。



该命令中“-t”指定线程，“200”指定攻击线程数(取值范围为：10～300)，“-s”指定地址源 IP 地址，“＊”隐藏攻击源 IP 地址。192.168.6.160 是被攻击计算机 B 的地址。

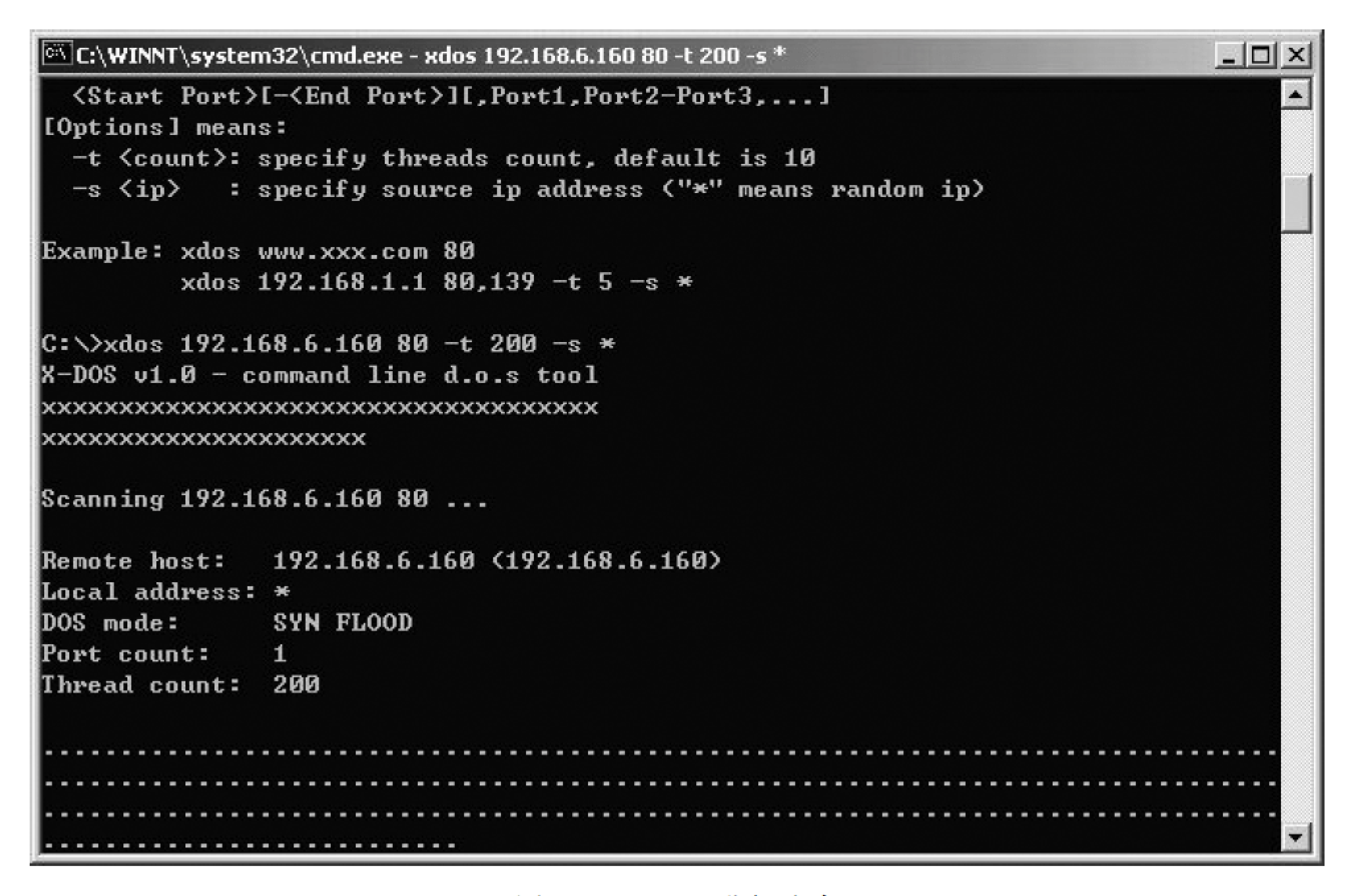


图 3-11　xdos 进行攻击

(5) 在被攻击计算机 B 中可以看到计算机的处理速度明显下降，甚至瘫痪死机，鼠标指针已无法移动。在 Sniffer Pro 的 Traffic Map 视图中可看到大量伪造 IP 的主机请求与计算机 B 建立连接，如图 3-12 所示。

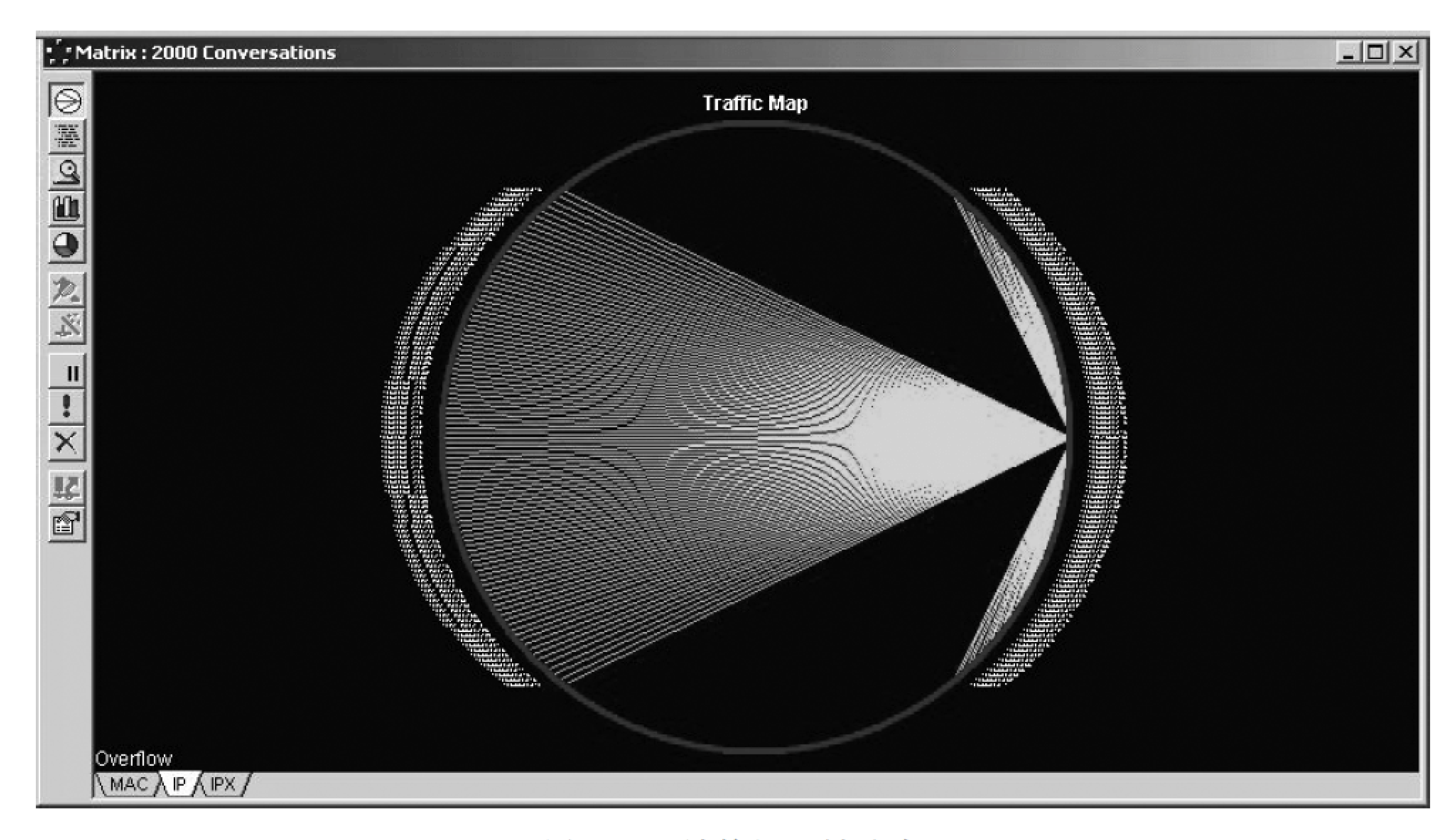


图 3-12　计算机 B 被攻击

(6) 计算机 A 停止攻击后，被攻击的计算机 B 恢复快速响应。图 3-13 所示为受攻击前



的报文统计：捕获报文数为 1KB 时，捕获报文的数据缓冲区大小为 5%。图 3-14 所示为受攻击后的报文统计：捕获报文数约为 100KB 时，捕获报文的数据缓冲区大小为 100%，运行速度会下降直至瘫痪死机，并拒绝为合法的请求服务。

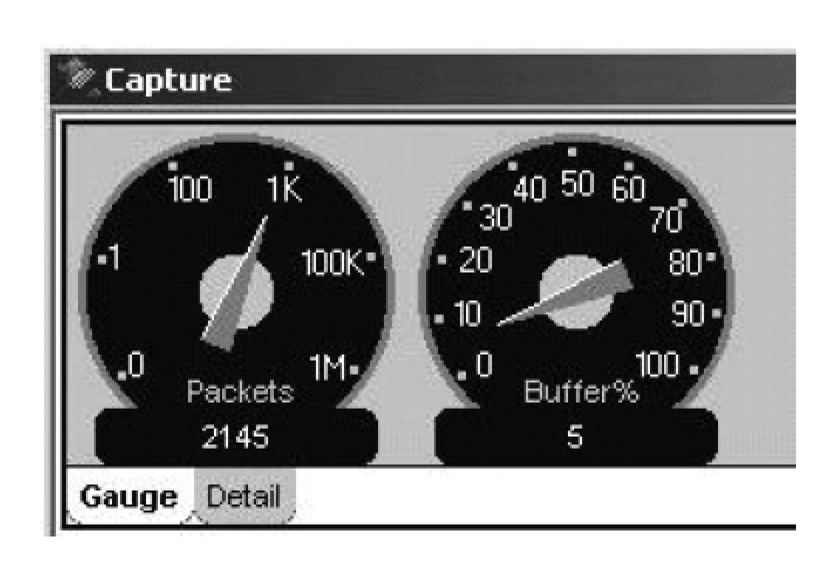


图 3-13　受攻击前的报文统计

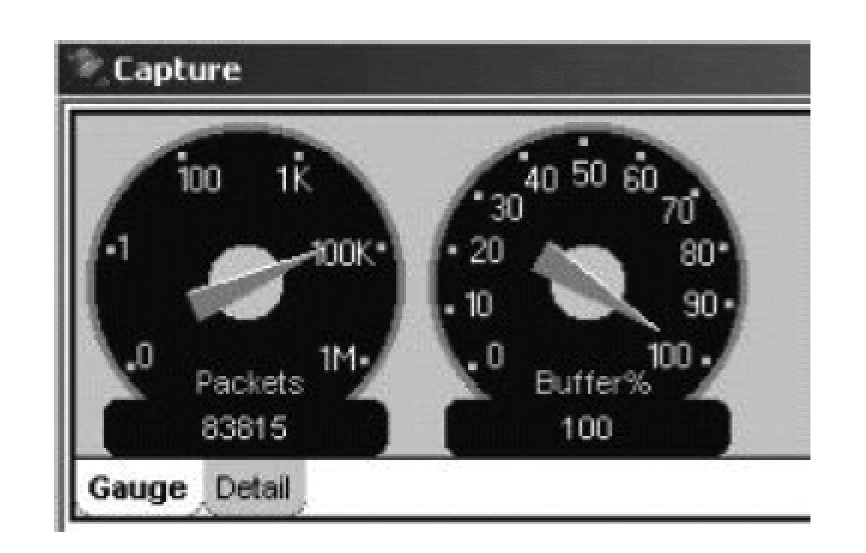


图 3-14　受攻击后的报文统计

3.3.2　防范方法

在 Windows 2000 中加固 TCP/IP 堆栈可以防范拒绝服务攻击，可以使用下列方法（同样适用于 Windows Server 2003 系统）：

(1) 使用最新的安全修复程序更新计算机。

(2) 在基于 Windows 2000 的工作站和服务器上加固 TCP/IP 协议堆栈。

(3) 默认的 TCP/IP 堆栈配置能够处理正常的 Internet 流量。如果将某台计算机直接连接到 Internet，则建议加固 TCP/IP 堆栈以抵御拒绝服务攻击。

3.4　习　　题

1. 黑客进行的网络攻击通常有哪些类型？
2. 简述黑客攻击的六个基本步骤。
3. 简述如何拒绝服务攻击及其后果。
4. 请问有了杀毒软件与防火墙，上网就安全了吗？
5. 试使用 X-Scan 扫描器进行端口扫描，分析扫描结果，从而加强系统的安全性。
6. 试使用 360 安全卫士进行系统漏洞扫描，查看并修复系统漏洞。



第4章　防　火　墙

本章学习目标

- 防火墙的基本概念和基本功能。
- 防火墙的种类及各种类型防火墙的基本特性。
- 主要防火墙技术及各自的工作原理和优缺点。
- 防火墙的体系结构。
- 防火墙的配置原则与防火墙的选择。
- 防火墙的基本配置方法。

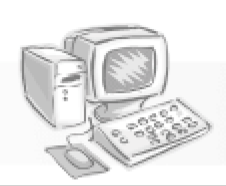
企业的内部网与互联网相连，其最大好处是方便企业内部之间、企业与外部之间的信息交流。然而，与互联网这样一个世界范围的开放网络连接，在获得利益的同时也要付出安全代价，因为互联网上的每个用户都可能访问企业网。如果没有一个安全保护措施，黑客很可能在不被察觉的情况下进入企业网，非法访问企业的资源，甚至恶意破坏企业网站(这就是平时常说的被黑客“黑”了)。

于是，各企业纷纷为自己的内部网络“筑墙”，防病毒与防黑客成为确保企业信息系统安全的基本目标。这里所说的“墙”在相当程度上指的就是“防火墙”，它是网络安全中最重要的设备之一，被誉为企事业单位局域网的网络守护神。

防火墙的主要用途就是根据所设定的规则对通信双方的数据包(主要是对非信任的外部网络)进行过滤。过滤规则中可能是对方的网络地址、IP 地址、计算机名、端口、通信协议和服务等。其最终目的就是过滤掉存在安全风险的通信数据包，如黑客攻击类的端口扫描数据包、Ping 测试包和拒绝服务类数据包等。但防火墙不能过滤计算机病毒、木马及恶意软件等的入侵和感染，防火墙只是整个企业安全防御系统中的一个重要环境。本章主要介绍防火墙的功能、主要技术以及在网络安全方面的具体应用。

4.1　防火墙概述

防火墙指隔离在内部网络与外部网络之间的一道防御系统，是这一类防范措施的总称。在互联网上防火墙是一种非常有效的网络安全模型，可以隔离风险区域(如互联网或有一定风险的其他网络)与安全区域(企业内部网)的连接，不会妨碍人们对风险区域的访问，而来自互联网的访问者必须通过防火墙的安全检查，才能访问内部网络的计算机。



4.1.1 防火墙定义

防火墙(Firewall)是目前最重要的一种网络安全防护设备,在网络中经常以图 4-1 所示的两种图标出现。左边图标非常形象,真正像一堵墙堵住了火的蔓延;而右边那个图标则是从防火墙的过滤机制形象化来的,它是一个二极管图标。

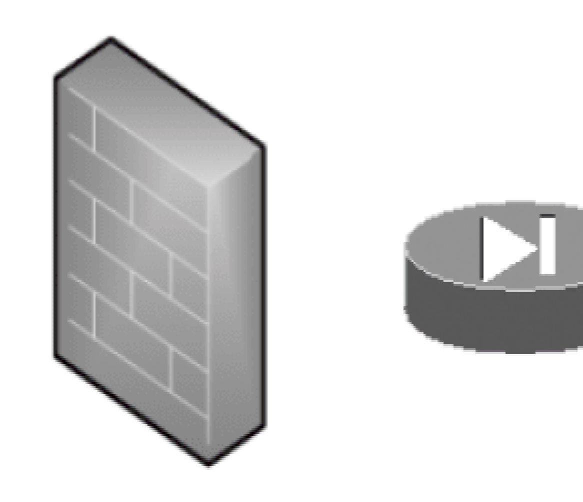


图 4-1 防火墙图标

防火墙最初的用途不是为了网络安全,而是为了控制实际的火灾。古代构筑和使用木质结构房屋的时候,为防止火灾的发生和蔓延,人们将坚固的石块堆砌在房屋周围作为屏障,这种防护构筑物就被称为“防火墙”。其实与防火墙一起起作用的是“门”,如果没有门,各房间的人如何沟通呢?住在这些房间的人如何进出呢?当火灾发生时,这些人又如何逃离现场呢?这个门就相当于这里所讲的防火墙的“安全策略”,也就是安全过滤机制。所以防火墙并不是一堵实心墙,而是带有一些小孔的墙,这些小孔用来留给那些允许进行的通信。在这些小孔中安装的过滤机制,只有符合条件的通信才能通过。

现在,当我们谈及网络安全时,“防火墙”这个术语意味着不同的概念,但其基本含义是:防火墙用来保护我们的网络免受恶意人员的攻击,并在定义的边界点(防火墙)停止他们的非法行为。因此,防火墙指的是隔离在内部网络与外界网络之间的,控制介于网络不同区域的通信的一台设备或者一套防御系统。在简单的小型网络设计中,比如在普通家庭环境中,通常使用一台设备(如 Cisco 的无线 Linksys 路由器)来实现这些功能。而在大型的企业网络中,防火墙包括很多组件,比如边界防火墙、状态防火墙、VPN、IDS 系统以及其他组件。通常人们将包括很多组件的防火墙称作防火墙系统。防火墙可以使企业内部网络与 Internet 之间或者与其他外部网络互相隔离,通过限制网络互访来保护内部网络。

防火墙最初的设计思想是对内部网络总是信任的,而对外部网络却总是不信任的,所以最初的防火墙只是对外部进来的通信进行过滤,而对内部网络用户发出的信息不作限制。然而,绝大多数(占 60%~70%)的网络威胁和攻击发生在网络内部,主要来自公司内部的雇员。目前最新的分布式防火墙系统在过滤机制上已有所改变,不仅对外部网络发来的通信连接进行过滤,对内部网络用户发出的部分连接请求和数据包同样进行过滤。

4.1.2 防火墙的主要功能

防火墙的作用是流量过滤,防止不希望的非法流量和未经过授权的流量进出被保护的网络。防火墙的任务是通过各种端口辨别从外部不安全网络发送到内部安全网络中的计算机数据是否有害,尽可能对有害数据进行报警和拦截,从而保障网络系统安全。安装防火墙和正确配置后一般可以达到以下目的。

1. 强化安全策略,保障网络的安全

防火墙通过仅允许“认可的”和符合规则的请求通过的方式来强化安全策略,过滤不安



全的服务。由于只有经过精心选择的应用协议才能通过防火墙，所以网络安全会得到保障。

2. 控制存取

指依据管理者所设定的存取控制，决定网络信息的许可或者拒绝，存取控制的条件包括资料封包的来源地址、目标地址、连接的网络服务协议种类以及使用者的身份等。存取控制甚至可以做到控制网络服务的某些特定指令是否允许其执行。

3. 控制对特殊站点的访问

防火墙能控制对特殊站点的访问，如有些主机能被外部网络访问而有些则要被保护起来。

4. 安全策略的检查和集中化的安全管理

如果使用了防火墙，所有信息都必须经过防火墙，防火墙就成为一个安全检查点，同时可以将安全软件都放在防火墙上集中管理。

5. 对网络访问进行记录和统计

如果所有对 Internet 的访问都经过防火墙，那么，防火墙就能记录下这些访问，并能提供网络使用情况的统计数据。当发生可疑操作时，防火墙能够报警并提供网络是否受到监测和攻击的详细信息。

6. 隐藏用户站点或网络拓扑并防止内部信息的外泄

通过防火墙对内部网络的划分，可实现对内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。

4.1.3 与防火墙有关的主要术语

在继续下面具体的防火墙技术和应用学习之前，需要对一些重要的术语有一些认识，这些术语将在本章后面的内容中用到。

1. 网关

网关是在两个设备之间提供转发服务的系统。网关的范围可以从互联网应用程序(如公共网关接口 CGI)到在两台主机间处理流量的防火墙网关。网关可以是软件的(如在 Windows 系统中配置的 ICS 就是通过设置网关而实现的)，也可以是硬件的(如语音网关、连接网关等)。

2. 电路级网关

电路级网关用来监控受信任的客户或服务器与不受信任的主机间的 TCP 握手信息，以此来决定该会话是否合法。有两种方法来实现这种类型的网关，一种是由一台主机充当筛选路由器，而另一台充当应用级防火墙；另一种方法是在第一个和第二个防火墙主机之间建立安全的连接，这种结构的好处是当一次攻击发生时能提供容错功能。

3．应用级网关

应用级网关可以工作在 OSI 七层模型的任一层上，能够检查进出的数据包，通过网关复制传递数据，防止受信任服务器和客户机与不受信任的主机直接建立连接。应用级网关能够理解应用层上的协议，能够做复杂一些的访问控制，并做精细的注册。这通常是在特殊的服务器上安装软件来实现的。

4．包过滤

包过滤是处理网络上基于 packet-y-packet（包到包）流量的设备。包过滤设备允许或阻止包，典型的实施方法是通过标准的路由器。包过滤技术是防火墙的主要技术之一，在本章后面具体介绍。

5．代理服务器

代理服务器可代表内部客户端与外部的服务器通信。代理服务器这个术语通常是指一个应用级的网关，虽然电路级网关也可作为代理服务器的一种。应用代理服务器技术也是防火墙的一种主要技术，也将在本章后面具体介绍。

6．网络地址转换

网络地址转换（Network Address Translation，NAT）是对 Internet 用户隐藏内部地址（一般称为私有地址），防止内部地址公开的一种技术。

7．堡垒主机

堡垒主机是一种被强化的可以防御进攻的计算机，被暴露于互联网之中，作为进入内部网络的一个检查点，以达到把整个网络的安全问题集中在某个主机上解决。

从堡垒主机的定义可以看出，它是网络中最容易受到侵害的主机，所以堡垒主机也必须是自身保护最完善的主机。一个堡垒主机通常使用两块网卡，分别连接内网和外网，如图 4-2 所示。

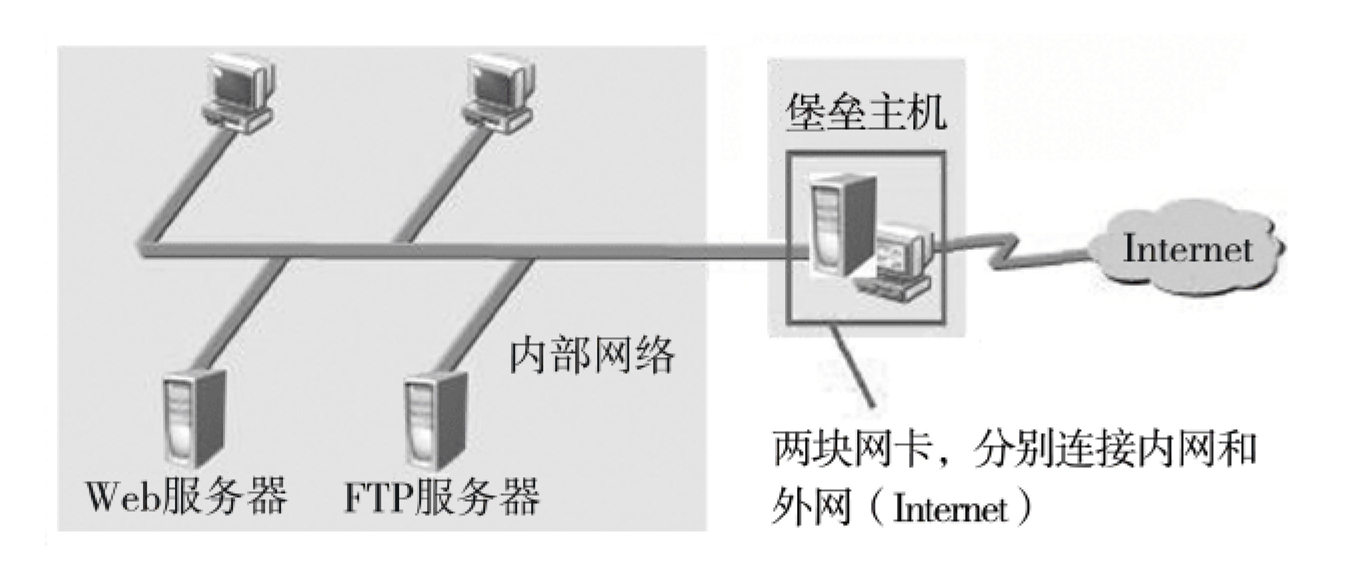


图 4-2 堡垒主机部署的位置

堡垒主机经常配置网关服务，网关服务是一个进程，用来提供从公网到私有网络的特殊协议路由；反之亦然。在一个应用级的网关里，想使用的每一个应用程序协议都需要一个进程。因此，想通过一台堡垒主机来路由 E-mail、Web 和 FTP 服务时，必须为每一个服务都提供一个守护进程。



8. 强化操作系统

防火墙要求尽可能只配置必需的少量的服务。为了加强操作系统的稳固性,防火墙安装程序要禁止或删除所有不需要的服务。

9. 非军事化区域(Demilitarized Zone,DMZ)

DMZ 是从企业内部网络中划分的一个小区域,存在于公司的内部网络和外部网络之间,如图 4-3 所示。

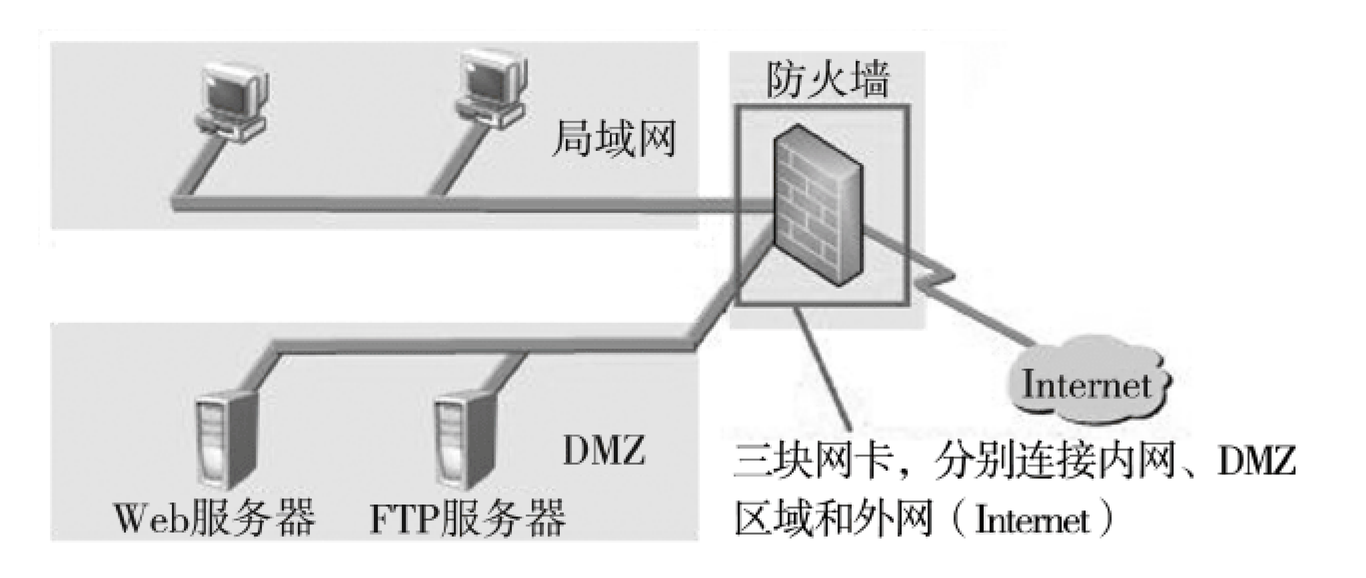


图 4-3　DMZ 部署的位置

DMZ 是内网和外网的一个缓冲区,在其中可包括内部网络中用于对外(如 Internet)提供公众服务的服务器,如 Web 服务器、邮件服务器、FTP 服务器、外部 DNS 服务器等,受保护的级别较低。因为如果级别太高,则这些提供公共服务的网络应用就无法进行。

4.2　防火墙的分类

认识了防火墙之后,我们就来对当前市场上的防火墙进行一下分类。目前市场上的防火墙产品非常多,划分的标准也比较杂。在此将主流的分类标准进行介绍。

4.2.1　按防火墙的软、硬件形式划分

如果从防火墙的软、硬件形式来分,防火墙可以分为硬件防火墙和软件防火墙。

1. 硬件防火墙

最初的防火墙与人们平时所看到的集线器、交换机一样,都属于硬件产品(在其中包含软件功能,如它的 IOS)。图 4-4 所示是 Cisco 公司的一款 PIX-515E-R-BUN 防火墙。一些高级的防火墙不仅可以连接多个内部局域网,还可连接多个外部网络。图 4-5 所示是一款多网络接口的硬件防火墙,它们在外观上与平常所见到的集线器和交换机类似。

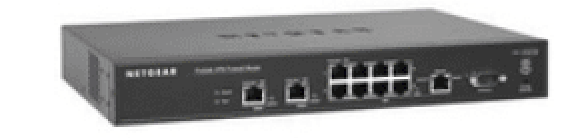
硬件防火墙有两种结构:一种是普通硬件级防火墙,这种防火墙措施相当于专门拿出一台计算机安装了软件防火墙,其安全性并不能做到最好。另一种是所谓的“芯片”级硬件防火墙,它采用专门设计的硬件平台,在上面搭建的软件也是专门开发的,可以达到较好的安全性能保障。

无论是哪种硬件防火墙,管理员都可以通过计算机连接上去设置其工作参数。对数据

吞吐量要求很高的网络里，档次低的防火墙仍然会形成瓶颈，所以对于一些大企业而言，芯片级的硬件防火墙才是他们的首选。




图 4-4　硬件防火墙示例


图 4-5　多网络接口的硬件防火墙

有人也许会这么想，既然 PC 架构的防火墙与一台 PC 机差不多，那么购买这种防火墙还不如自己配置一台多网卡计算机来做防火墙。虽然理论上可以这么做，但是工作效率并不能和真正的 PC 架构防火墙相比，因为 PC 架构防火墙采用的是专门修改简化过的系统和相应防火墙程序，比一般计算机系统和软件防火墙结合更加紧密。而且由于它的工作性质决定了它要具备非常高的稳定性、实用性和非常高的系统吞吐性能，这些要求并不是安装了多网卡的计算机就能简单替代的。

目前能开发、生产硬件防火墙产品的厂家并不多，国内、外比较著名的防火墙品牌有：Cisco、Juniper、Watchguard、飞塔（Fortigate）、华为 3COM（H3C）、东软（Neusoft）、锐捷（Ruijie）、合勤（ZyXEL）和神州数码等。

2. 软件防火墙

随着防火墙应用的逐步普及和计算机软件技术的发展，为了满足不同层次用户对防火墙技术的需求，许多网络安全软件厂商开发出了基于纯软件的防火墙，俗称“个人防火墙”，如天网防火墙、傲盾防火墙、金山毒霸防火墙、瑞星防火墙、ZoneAlarm 等。

软件防火墙是一种安装在负责内、外网络转换的网关服务器或者独立的个人计算机上的特殊程序。它是以逻辑形式存在的，防火墙程序跟随系统启动，通过运行在 Ring 0 级别的特殊驱动模块，把防御机制插入系统关于网络的处理部分和网络接口设备驱动之间，形成一种逻辑上的防御体系。

由于软件防火墙自身属于运行于系统上的程序，不可避免地需要占用一部分 CPU 资源以维持工作，而且由于数据判断处理需要一定的时间，在一些数据流量大的网络里，软件防火墙会使整个系统工作效率和数据吞吐速度下降，甚至有些软件防火墙会存在漏洞，导致有害数据可以绕过它的防御体系，给数据安全带来损失。因此，许多企业并不会考虑用软件防火墙方案作为公司网络的防御措施，而是使用看得见摸得着的硬件防火墙。

现在的防火墙产品也开始由最初的独立软件防火墙或者硬件防火墙，走向软、硬混合类型的混合类型防火墙。如最新的分布式（也称“嵌入式”）防火墙，就是同时有硬件防火墙设备和防火墙软件的混合类型防火墙系统。

4.2.2　按防火墙性能划分

在实际的应用中，用户通常是根据具体应用的安全和性能需求而选择不同性能等级的防火墙产品的。本节介绍从性能等级（其中还体现功能上的差异）上进行的分类。

1. 个人防火墙

个人防火墙通常为个人用户所选择，用于为个人计算机提供简单的防火墙功能。由于



永久 Internet 连接(与拨号连接相对)的数量不断增长,个人防火墙的使用也在增加。

虽然个人防火墙是为了保护单一个人计算机而设计的,但是如果安装它的计算机是与内部网络上的其他计算机共享到 Internet 的连接,则它也可以保护小型网络。但是,个人防火墙的性能有限,并会造成安装它的个人计算机的性能下降。这种保护机制通常不如专用防火墙解决方案有效,因为它们通常只限于阻止 IP 和端口地址。

2. 路由器防火墙

路由器通常支持前面所讨论的一个或多个防火墙功能。它们可以再细分成为低端和高端路由器。低端路由器提供了阻止和允许特定的 IP 地址和端口号的基本防火墙功能,以及使用 NAT 来隐藏内部 IP 地址。在高端路由器中,防火墙功能与硬件防火墙设备的功能类似,但是成本更低而且吞吐量也更低。

3. 低端硬件防火墙

硬件防火墙市场中的低端产品是需要一点或一点也不需要配置的即插即用设备,就像普通的桌面交换机一样。这些低档设备经常集成了交换机和(或)VPN 功能。低端硬件防火墙适合小型公司和在较大企业中内部使用。

4. 高端硬件防火墙

高端的硬件防火墙可以通过添加第二个作为热备用单元运行的防火墙,以获得可用性的提高。由于入侵经常发生,DoS 攻击、窃取和数据损坏始终在进行尝试,因此高端硬件防火墙单元应该部署在中心或总公司位置中。

5. 高端服务器防火墙

高端服务器防火墙将防火墙功能添加到高端服务器中,在标准软件和软件系统上提供可靠快速的保护。此方法的好处是使用熟悉的硬件或软件,这样可以减少库存项目,简化培训和管理,提供可靠性和扩展性。服务器防火墙适合在一些特殊的硬件或软件平台上有高投资的地方。

各类防火墙属性见表 4-1。

表 4-1 各类防火墙属性列表

防火墙属性	个人防火墙	路由器防火墙	低端硬件防火墙	高端硬件防火墙	高端服务器防火墙
受支持的基本功能	大多数个人防火墙支持静态数据包筛选器、NAT 和状态检查,有些个人防火墙支持线路层检查和(或)应用程序层筛选	大多数路由器防火墙支持静态数据包筛选器。低端路由器通常支持 NAT;高端路由器可能支持状态检查和应用程序层筛选	大多数低端硬件防火墙支持静态数据包筛选器和 NAT。可能支持状态检查和应用程序层筛选	大多数高端硬件防火墙支持静态数据包筛选器和 NAT。可能支持监控状态的检查和应用程序层筛选	大多数高端服务器防火墙支持静态数据包筛选器和 NAT。可能支持监控状态的检查和应用程序层筛选



续表

防火墙属性	个人防火墙	路由器防火墙	低端硬件防火墙	高端硬件防火墙	高端服务器防火墙
配置	自动（有手动选项）	通常在低端路由器上是自动的，在高端路由器上是手动的	自动（有手动选项）	通常手动	通常手动
阻止或允许 IP 地址	是	是	是	是	是
阻止或允许协议/端口号	是	是	是	是	是
阻止或允许传入的 ICMP 消息	是	是	是	是	是
控制传出的访问	是	是	是	是	是
应用程序保护	可能	可能	没有	默认支持	默认支持
声响或可见警报	可能	通常	没有	是	是
攻击的日志文件	可能	在许多情况下	没有	是	是
实时警报	取决于产品	在许多情况下	没有	是	是
VPN 支持	没有	经常在低端路由器中，在高端路由器中不常见。用于此任务的通常是单独的专用设备或服务器	可能	默认支持	默认支持
远程管理	没有	是	是	是	是
制造商支持	取决于产品	通常在低端路由器中受到限制，但在高端路由器中可用	有限	很好	很好
高可用性选项可用	否	低端：否；高端：是	没有	是	是
并发会话的个数	1～10	10～1000	10～7500	7500～500 000	大于 50 000（可跨越多个网段）
模块式升级（硬件或软件）	没有限制	低端：否；高端：有限	有限	是	是（使用常用操作系统）
价格范围	低（在很多情况下免费）	从低到高	低	高	高
主要优点	便宜，易于管理	低成本解决方案，可以整合配置，投资保护	成本低，配置简单	模块化系统，远程管理，适应性好，应用程序层筛选	高性能，整合服务，可用性、适应性和可扩展性好
主要缺点	集中管理比较困难，仅具有基本控制，性能限制	功能有限，仅具有基本控制，影响性能	功能有限，吞吐量有限，有限的制造商支持	成本高，配置和管理复杂	要求高端硬件，容易遭受攻击



4.3 主要防火墙技术

一个防火墙系统可能由很多不同的设备和组件组成,其中一部分组件的作用就是流量过滤,这部分组件就是大多数人称为防火墙的部分。防火墙的过滤技术有很多种不同的过滤方式,但主要有三种:包过滤技术、应用代理技术和状态检测技术。采用包过滤技术和状态检测技术统称为网关型防火墙,以以色列的CheckPoint防火墙和Cisco公司的PIX防火墙为代表;采用应用代理技术的防火墙以美国NAI公司的Gauntlet防火墙为代表。这些采用不同技术的防火墙在功能和设计上不同,并且在网络架构中的用法也不同。

4.3.1 包过滤技术

防火墙的包过滤(Packet filtering)功能是在网络中的网络层和传输层中实现的。它是根据分组包的源/宿地址、端口号及协议类型、标志确定是否允许分组包通过,只有满足过滤逻辑的数据包才被转发到相应的目的地出口端,其余数据包则被从数据流中丢弃。而这些信息来源就是IP、TCP或UDP数据包的包头。

1. 包过滤防火墙原理

包过滤防火墙一般在路由器上实现,用以过滤用户定义的内容,如IP地址。其工作原理是:系统在网络层检查数据包,与应用层无关。这样系统就具有很好的传输性能,可扩展能力强。但是,包过滤防火墙的安全性有一定的缺陷,因为系统对应用层信息无感知,也就是说,防火墙不理解通信的内容,所以可能被黑客所攻破。图4-6所示为包过滤防火墙工作原理图。

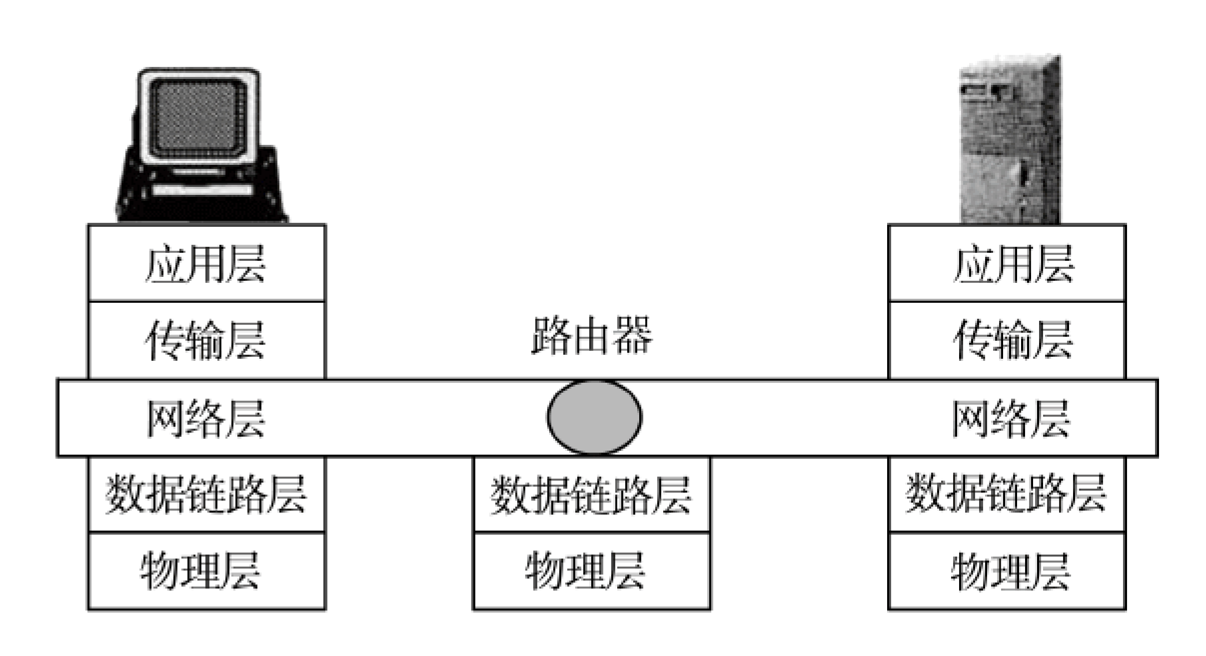


图4-6 包过滤防火墙工作原理图

2. 包过滤技术的主要优、缺点

包过滤防火墙主要部署在组织的边缘,进行粗度过滤。由于其只检查目的端口和(或)源/目的IP地址,因此具有速度快的优点;一旦知道了必须的端口和(或)子网,就可以在几分钟之内设置好包过滤防火墙,没有复杂的规则设置,具有快速部署的优点。

但是,因为包过滤防火墙只做简单的包检测,所以其安全性较低;包过滤防火墙不能阻

止应用层的攻击；大多数过滤防火墙中缺少审计和报警机制，且管理方式和用户界面较差。

4.3.2　应用代理技术

应用代理（Application Proxy）防火墙也叫应用网关（Application Gateway），是内部网与外部网的隔离点，起着监视和隔绝应用层通信流的作用。它工作在OSI模型的最高层（应用层），掌握着应用系统中可用做安全决策的全部信息。其特点是完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。

这种防火墙针对每种应用协议提供相应的代理服务，经由代理服务器（代理主机）访问内、外部网络，并将结果返回给代理客户端，其体系结构如图4-7所示。代理服务器技术是防火墙技术中最受推崇的一种安全技术措施，它可以将被保护的网络内部结构屏蔽起来，增强网络的安全性能，同时可以用于实施较强的数据流监控、过滤、记录和报告等功能。

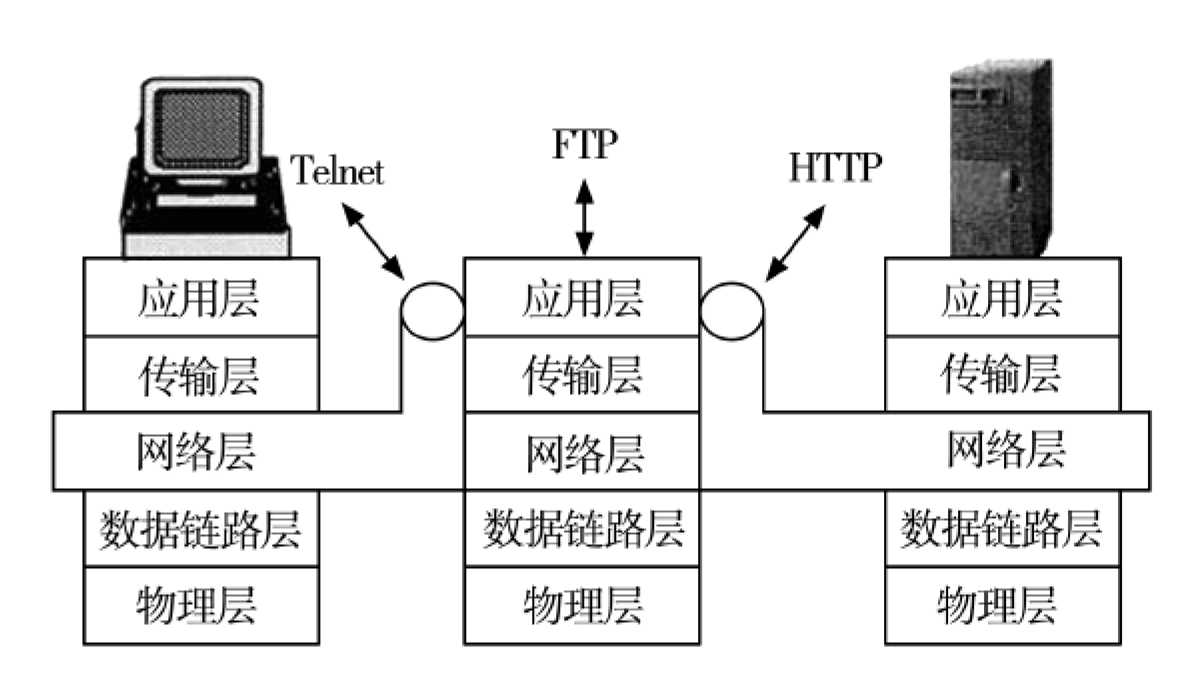


图4-7　应用代理防火墙工作原理图

1. 应用代理防火墙的工作原理

代理服务器防火墙检查所有应用层的信息包，并将检查的内容信息放入决策过程，从而提高网络的安全性。然而，应用网关防火墙是通过打破客户机/服务器模式实现的。每个客户机/服务器通信需要两个连接：一个是从客户端到防火墙，另一个是从防火墙到服务器。另外，每个代理需要一个不同的应用进程，或一个后台运行的服务程序，对每个新的应用必须添加针对此应用的服务程序，否则不能使用该服务。图4-7所示为代理服务器防火墙工作原理图。

2. 应用代理技术的性能特点

提供的安全级别高于包过滤型防火墙；可以配置成唯一的可被外部看见的主机，以保护内部主机免受外部攻击；可以强制执行用户认证；能提供较详细的审计日志；速度比包过滤慢。

4.3.3　状态检测技术

状态检测防火墙的安全特性非常好，它采用了一个在网关上执行网络安全策略的软件引擎，称之为检测模块。检测模块在不影响网络正常工作的前提下，采用抽取相关数据的方



法对网络通信的各层实施监测，抽取部分数据，即状态信息，并动态地保存起来。

一个有状态包检查的防火墙跟踪的不仅是包中包含的信息。为了跟踪包的状态，防火墙还记录有用的信息以帮助识别包，如已有的网络连接、数据的传出请求等。

1. 状态检测防火墙的工作原理

状态监视器防火墙克服了前两种防火墙技术的限制，它在不断开客户机/服务器的模式的前提下，提供一个完全的应用层感知。在状态监视器防火墙里，信息包在网络层就被截取了，然后防火墙从接收到的数据包中提取与安全策略相关的状态信息，并将这些信息保存在一个动态状态表中，用于验证后续的连接请求。可见，状态监视器防火墙提供了一个高安全性的方案，系统的执行效率提高了，还具有很好的可伸缩性和可扩展性。如图 4-8 所示为状态监视器防火墙工作原理图。

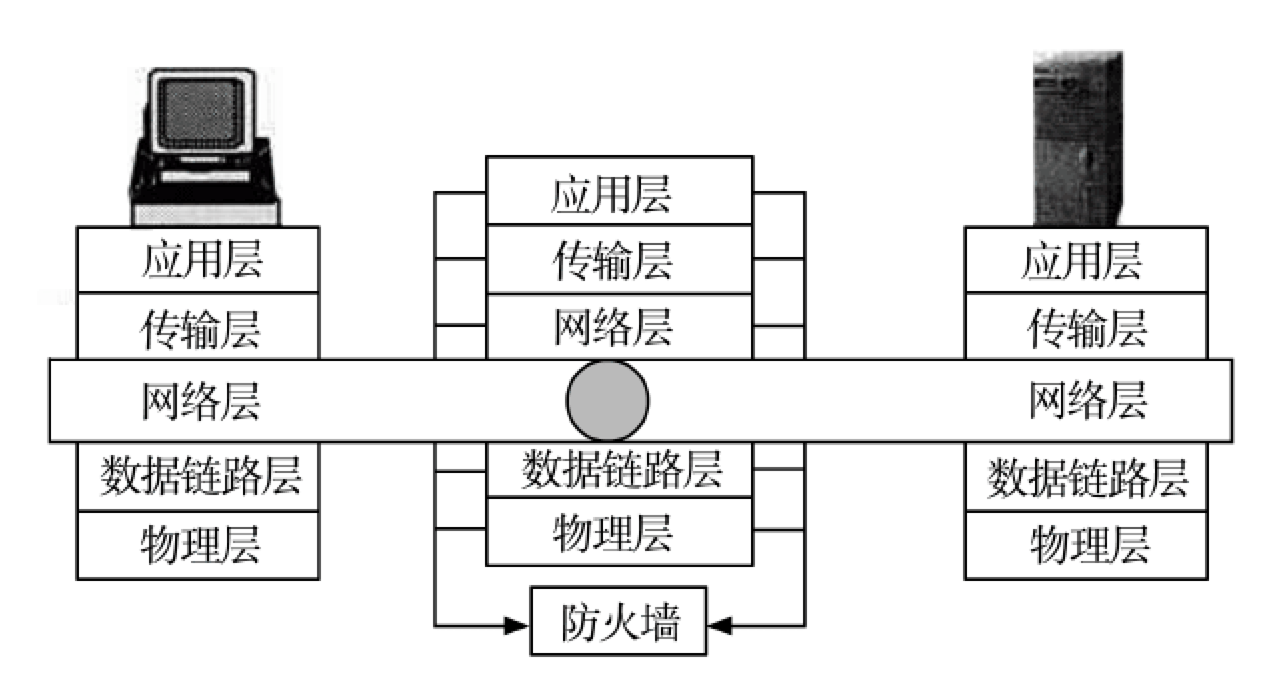


图 4-8　状态检测防火墙工作原理图

2. 状态监视器防火墙的特点

状态监视器防火墙的优点是：具备检查 IP 包的每个字段的能力，并遵从基于包中信息的过滤规则，很容易实现应用和服务的扩充；监测 RPC 和 UDP 之类的端口信息（而包过滤和代理网关都不支持此类端口）；具有基于应用程序信息验证一个包状态的能力。

但是，其配置非常复杂，且对数据包的记录、测试和分析工作可能会造成网络连接的某种迟滞。

三种类型防火墙的比较见表 4-2。

表 4-2　三种类型防火墙的比较

类　型	包 过 滤 型	代　理　型	状态检测型
优点	①速度快 ②防火墙是透明的，用户端不需要进行设置	①针对应用层数据进行过滤，增强了可控性 ②日志功能加强了对不安全因素的追踪与排查 ③屏蔽了内网细节	①减少了传统的包过滤防火墙的大量开放端口等一些安全问题 ②降低了管理员配置访问规则的难度
缺点	①无法过滤审核数据包的内容 ②无法详细记录细致的日志	①速度较慢 ②新的网络协议和应用都需要一套代理程序	①无法过滤审核数据包的内容 ②无法详细记录细致的日志



4.4　防火墙的体系结构

4.4.1　双宿主堡垒主机体系结构

双宿主堡垒主机体系结构提供来自于多个网络相连的主机的服务，它围绕双重宿主堡垒主机构筑。该双重宿主计算机位于互联网与内部网之间，至少有两个网络接口，且互联网和内部网都可以和它通信，但外部网络和内部网络之间不能直接通信。它相当于内部网络和外部网络的桥梁，能够提供较高级别的控制，可以完全禁止外部网络对内部网络的访问。

该体系结构比较简单，如图 4-9 所示。它可以允许用户登录到双重宿主主机，进而访问外部网络。但这种网络体系并不安全，因为在这种体系结构中主机被用作机构的单一入口点，如果一些不怀好意的人利用双重宿主主机自身的安全漏洞、病毒感染或种植木马将主机攻破，那么该主机就成了一个路由器，甚至可以通过该主机对网络进行重新设置。另外，该体系结构中用户访问互联网的速度会较慢。

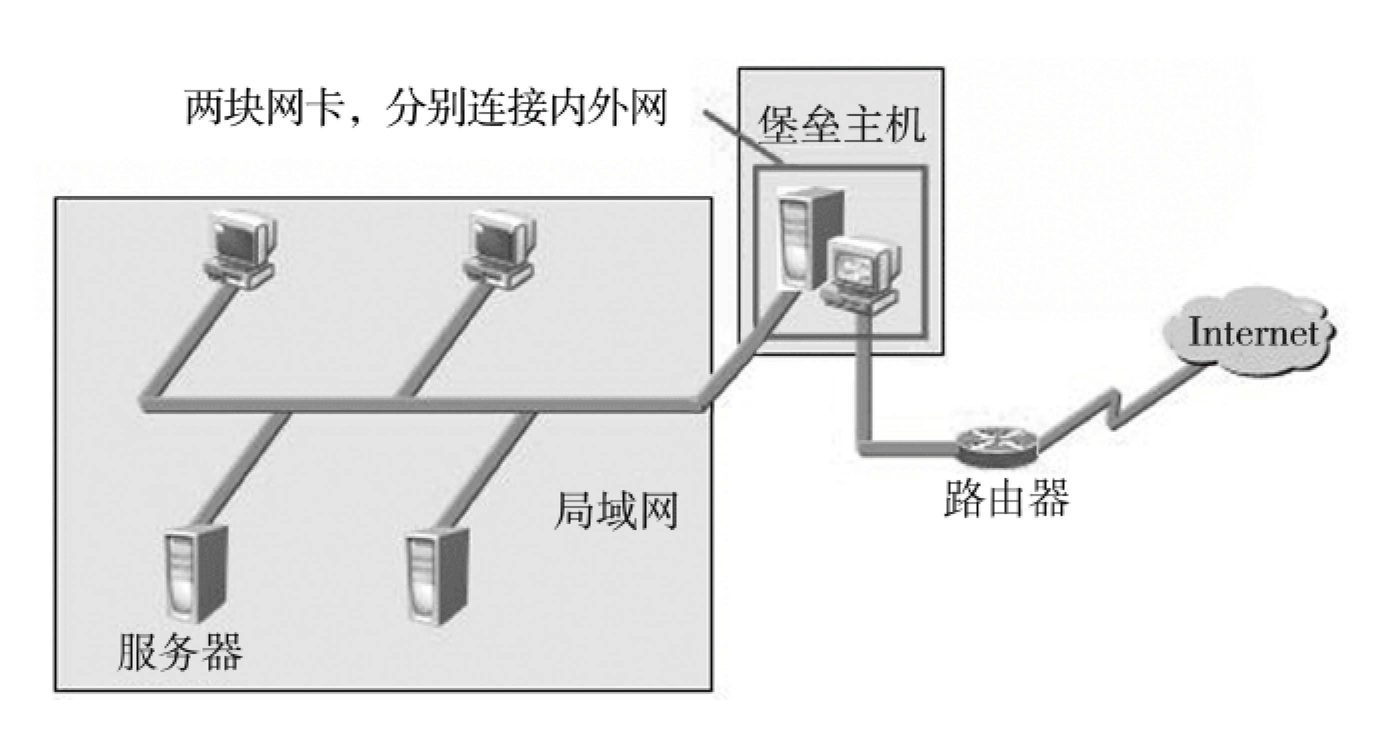


图 4-9　双重宿主主机体系结构

4.4.2　被屏蔽主机体系结构

被屏蔽主机体系结构防火墙使用一个路由器把内部网络和外部网络隔离开，其体系结构如图 4-10 所示。该体系结构中安全主要由数据包过滤提供，其中包括堡垒主机。堡垒主机是外网主机唯一能连接到内网的主机系统，任何外网的系统要访问内网的主机或服务器都必须先连接到这台堡垒主机上。在屏蔽路由上设置数据包过滤策略，让所有的外部连接只能到达内部堡垒主机。该结构比双重宿主堡垒主机体系结构更具有可用性和安全性，结构也相对较复杂。

该结构与双重宿主主机体系机构最大的差别是将路由器添加在主机和 Internet 之间用来进行 IP 数据包过滤，而该路由器将堡垒主机屏蔽。



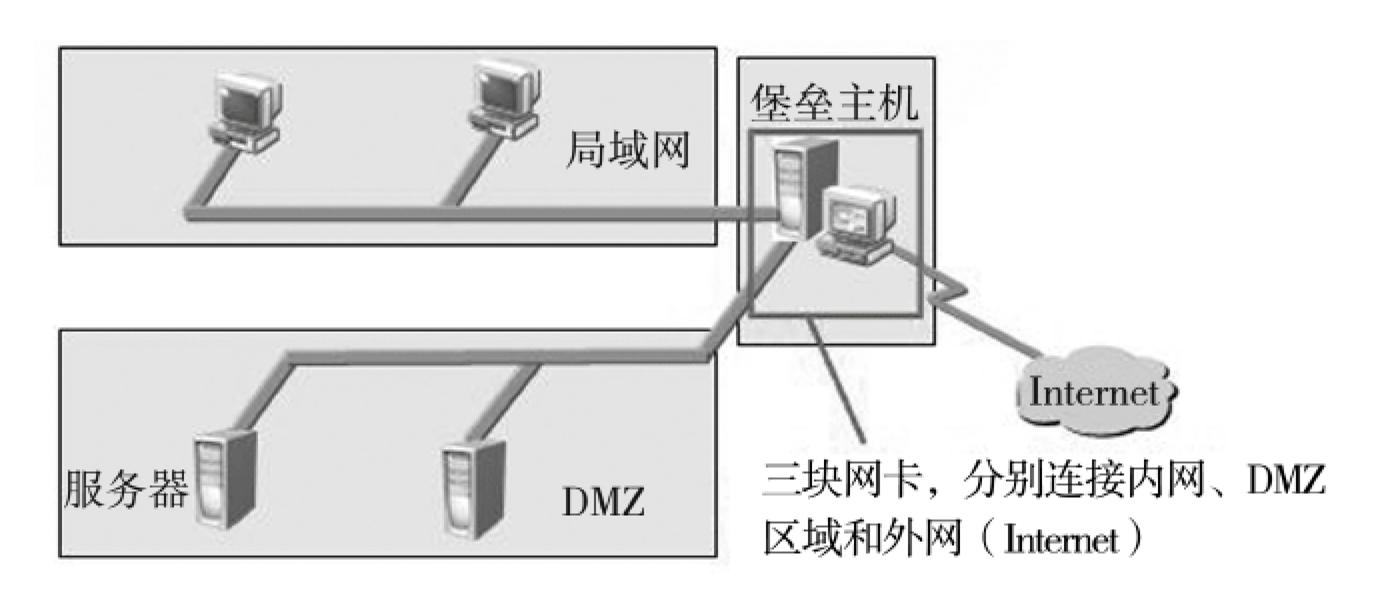


图 4-10　被屏蔽主机体系结构

4.4.3　被屏蔽子网体系结构

被屏蔽子网体系结构将额外的安全层添加到被屏蔽主机体系结构，增加了安全层的被屏蔽子网体系结构，如图 4-11 所示。它通过添加周边网络更进一步地把内网和外网隔离开。这个周边网络充当了内外网的缓冲区，称作“非军事区”(DMZ)。最简单的被屏蔽子网体系结构的形式是两个屏蔽路由器，一个连接到 DMZ 和内网之间，另一个连接到 DMZ 和外网之间。

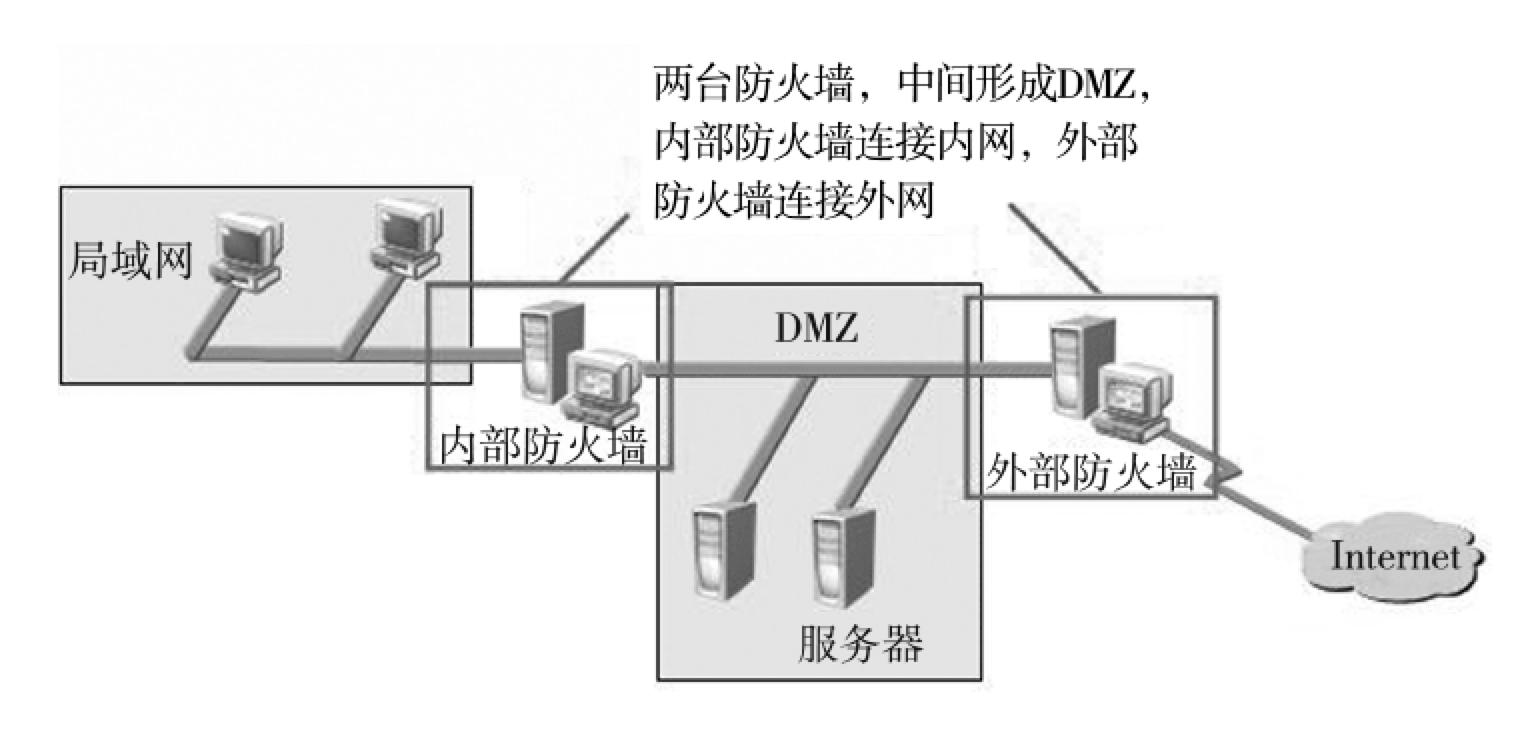


图 4-11　被屏蔽子网体系结构

4.5　防火墙配置的基本原则

防火墙的具体配置方法不是千篇一律的，即使是同一品牌的不同型号也不完全一样。在默认情况下，所有的防火墙都可按以下两种方式进行配置：

(1) 拒绝所有的流量。这需要在自己的网络中特别指定能够进入和出去的流量类型，大多数防火墙默认都是拒绝所有的流量作为安全选项。配置方法就是先全面禁止所有流量，然后对需要的某种应用进行单独设置。例如，如果想让自己的员工能够发送和接收 E-mail，就必须在防火墙上设置相应的规则，开启允许 POP3 和 SMTP 的进程。

(2) 允许所有的流量。这需要用户特别指定要拒绝的流量的类型。配置方法是先设置允许可通过的所有流量，然后再对不允许通过的流量进行禁止。这种配置方式的安全性不高。

在防火墙的配置中，首先要遵循的原则就是安全实用，从这个角度考虑，在防火墙的配置过程中需坚持以下三个基本原则。

1. 简单实用

越简单的实现方式，越容易理解和使用，越不容易出错，管理起来也越可靠和简便。

防火墙产品的初衷就是实现网络之间的安全控制，随着技术的成熟和发展，防火墙增加了查杀病毒、入侵检测等功能。这些增值功能并不是所有应用环境都需要，在配置时也可针对具体应用环境进行。

2. 全面深入

单一的防御措施难以保障系统的安全，只有采用全面的、多层次的深层防御战略体系，才能实现系统的真正安全。如一方面采用集互联网边界防火墙、部门边界防火墙和主机防火墙于一体的层次防御，另一方面将入侵检测、网络加密、病毒查杀等多种安全措施结合在一起的多层安全体系。

3. 内外兼顾

防火墙的一个特点是防外不防内，其实在现实网络环境中，70%以上的威胁都来自内部，所以我们要树立全面防护的观念，部署与其他安全措施（如入侵检测、主机防护、漏洞扫描、病毒查杀等）一起联动的机制。目前来说，要做到这一点还比较困难。

4.6　防火墙的选择

在市场上，防火墙的售价极为悬殊，从几百元到数十万元。因为各用户使用的安全程度不尽相同，因此厂商所推出的产品也有所区分。如何选择一个安全、实惠、合适的防火墙？面对种类繁多的防火墙产品，用户需要考虑如下的因素。

1. 考虑防火墙的基本功能

如果用户需要NNTP（Network News Transfer Protocol，网络消息传输协议）、XWindow、HTTP和Gopher等服务，防火墙应该包含相应的代理服务程序，也应具有集中邮件的功能，以减少SMTP服务器和外界服务器的直接连接，集中处理整个站点的电子邮件。

2. 考虑防火墙的可靠性

防火墙也是网络上的主机之一，也可能存在安全问题，防火墙如果不能确保自身安全，则其控制功能再强也不能完全保护内部网络。当黑客取得了防火墙上的控制权以后，几乎可为所欲为地修改防火墙上的访问规则，进而侵入更多的系统。因此防火墙自身应有相当高的安全保护。



3. 考虑用户的特殊要求

不同的用户往往有各自特殊的需求，不是每一个防火墙都会提供的，这成为选择防火墙的考虑因素之一，常见的需求如下。

(1) 网络地址转换功能(NAT)。进行地址转换有两个好处：其一是隐藏内部网络真正的 IP，使黑客无法直接攻击内部网络；其二可以让内部使用保留的 IP，这对许多 IP 不足的用户是有益的。

(2) 双重 DNS。当内部网络使用没有注册的 IP 地址，或是防火墙进行 IP 转换时，DNS 也必须经过转换，因为同一主机的内部 IP 与给予外界的 IP 将会不同，有的防火墙会提供双重 DNS，有的则必须在不同主机上各安装一个 DNS。

(3) 虚拟专用网络(VPN)。VPN 可以在防火墙与防火墙或移动的客户端之间对所有网络传输的内容加密，建立一个虚拟通道，让两者感觉是在同一个网络上，可以安全且不受拘束地互相存取。

(4) 杀毒功能。大部分防火墙都可以与防病毒软件搭配实现杀毒功能，有的防火墙则可以直接集成杀毒功能，差别只是杀毒工作是由防火墙完成，或是由另一台专用的计算机完成。

(5) 特殊控制需求。有时候企业会有特别的控制需求，如限制特定使用者才能发送 E-mail，FTP 只能下载文件不能上传文件，限制同时上网人数，限制使用时间或阻塞 Java、ActiveX 控件等，根据需求不同而定。

4. 考虑用户网络的规模

(1) 对于 ISP、网站等用户来说，由于其数据流量大，对速度和稳定性要求较高，如果这些用户需要在外部网络发布 Web(将 Web 服务器置于外部)，同时需要保护数据库或应用服务器(置于防火墙内)，这就要求所采用的防火墙具有传送 SQL 数据的功能，建议这些用户采用高效的包过滤型并且只允许外部 Web 服务器和内部传送 SQL 数据使用、100MB 及以上带宽的硬件防火墙。

(2) 对于大中型企业、金融、保险、政府等机构，共同之处在于网络流量虽然不是很大，但其内部数据比较重要，因此在选购防火墙时首要考虑的就是安全性问题。防火墙至少要能够将内部网分成两部分，即内部存放重要数据的网络与存放可提供外部访问数据的网络的分离。对于重要数据的传送，防火墙必须要有加密的 VPN 通信。

(3) 中小企业接入 Internet 的目的一般是为了方便内部用户浏览 Web、收发 E-mail 以及发布主页。这类用户在选购防火墙时，要注意考虑保护内部(敏感)数据的安全。建议这类用户选用一般的代理防火墙，具有 HTTP、E-mail 等代理功能即可。

(4) 对于普通用户，采用一般的个人软件防火墙就能满足实际的需要了。比如 Windows 防火墙、瑞星个人防火墙等。

随着人们对防火墙的不断重视，防火墙技术日趋成熟，全球有众多公司或科研机构通过对防火墙技术的不断研究，成功研制并开发出了自己的防火墙系统。在国外，著名的硬件防火墙有 Cisco、Juniper Netscreen 等，软件防火墙有微软的 ISA Server 2006 等。在国内，近来的防火墙技术也得到了飞速的发展，多家公司或科研机构也研制开发出了自己的防火墙



系统，如华为 Eudemon 防火墙、联想网御防火墙和方正方御防火墙，大部分通过了国家公安部等机构的测试，深受人们喜爱。

4.7　Windows 防火墙

Windows XP SP2(Service Pack 2)内置新的 Windows 防火墙，它取代了 ICF(Internet Connection Firewall，Internet 连接防火墙)。Windows 防火墙是一个基于主机的状态防火墙，它会断开非请求的传入通信，这些通信指并非为响应计算机的请求而发送的通信(请求通信)或被指定为可允许的非请求通信(例外通信)。Windows 防火墙针对依靠非请求传入通信攻击网络计算机的恶意用户和程序提供了一定程度的保护。

在这一节，主要掌握 Windows 防火墙的一般设置方法，利用 Windows 防火墙拦截某些端口、打开防火墙默认拦截的某些端口。

4.7.1　Windows 防火墙的一般设置方法

1. 启用 Windows 防火墙

右击桌面上“网上邻居”图标，在弹出菜单中选择【属性】命令，出现【网络连接】窗口。在窗口中右击【本地连接】图标，在弹出菜单中选择【属性】命令，出现【本地连接 属性】对话框，选择【高级】选项卡，如图 4-12 所示。



图 4-12　【本地连接 属性】对话框

单击【高级】选项卡上的【设置】按钮，弹出【Windows 防火墙】对话框，选择【常规】选项卡，选择【启用】选项，再单击【确定】按钮，启用 Windows XP 内置的防火墙，如图 4-13 所示。

【Windows 防火墙】对话框包括下列选项卡：常规、例外和高级。



1)【常规】选项卡

【常规】选项卡及其默认设置显示在图 4-13 中。在【常规】选项卡中,可以进行下列选择。

(1) 启用(推荐)。选择该项,对【高级】选项卡中选定的所有网络连接启用 Windows 防火墙。启用 Windows 防火墙后将只允许请求的和例外的传入通信,例外通信在【例外】选项卡中进行配置。

如果选择【启用(推荐)】单选按钮,则可以选中【不允许例外】复选框。选中该选项将只允许请求的传入通信。不管【高级】选项卡中的设置如何,【例外】选项卡中的设置将被忽略,所有的网络连接都将得到保护。

(2) 关闭(不推荐)。选择该选项,将禁用 Windows 防火墙。不推荐使用此选项,尤其是对于可以直接从 Internet 进行访问的网络连接,除非已经使用了第三方的主机防火墙产品。

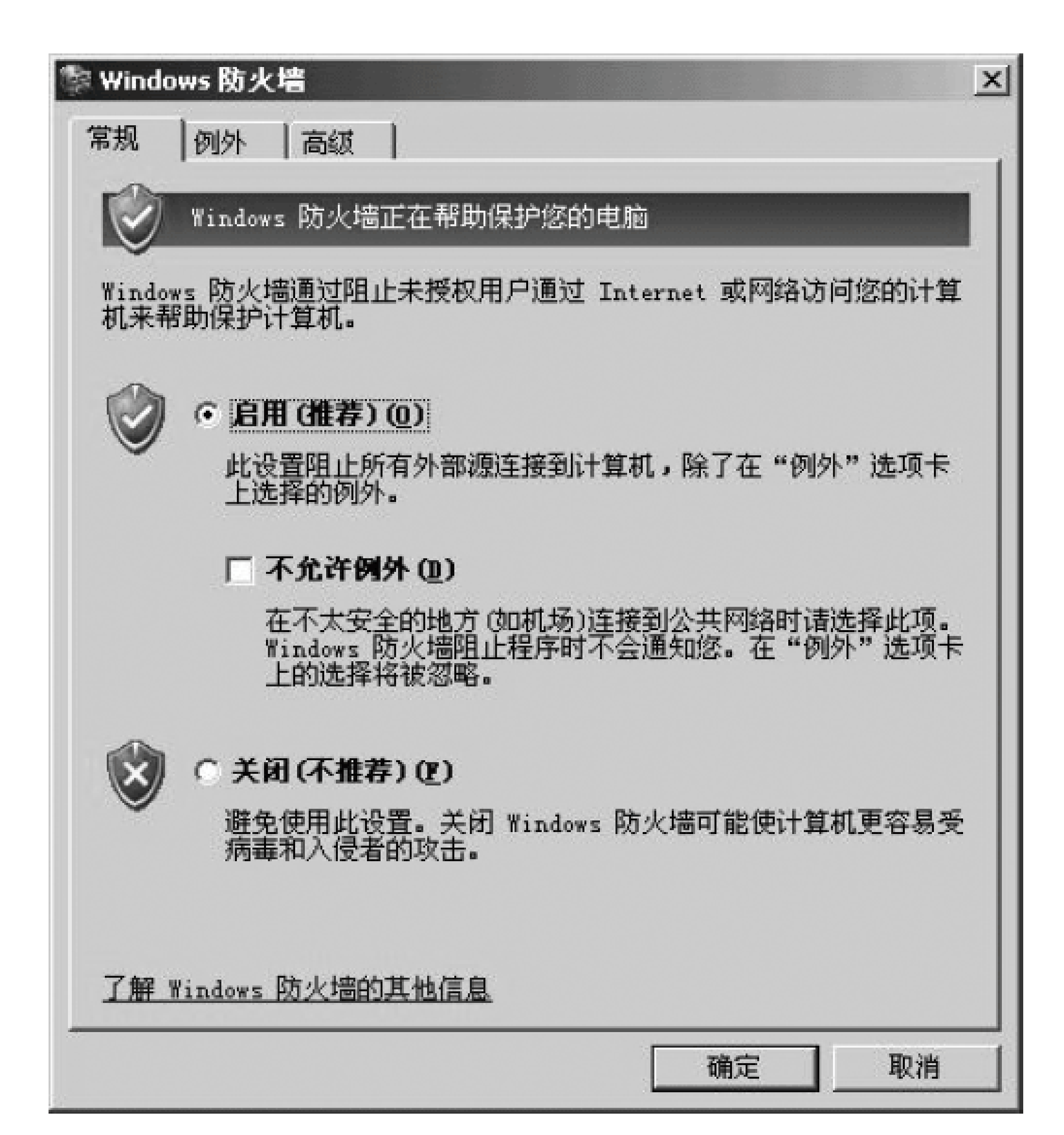


图 4-13 【Windows 防火墙】对话框

注意:对于所有运行带有 SP2 的 Windows XP 的计算机连接和新创建的连接,Windows 防火墙的默认设置都是选中【启用(推荐)】单选按钮。这会影响那些依赖非请求传入通信的程序或服务的通信。在这种情况下,必须识别出哪些程序不再运行,并且将这些程序或其通信添加为例外通信。许多程序,诸如 Internet 浏览器和电子邮件客户端(如 Outlook Express),并不依赖非请求通信,并且可以在 Windows 防火墙启用时正常运行。

2)【例外】选项卡

【例外】选项卡及其默认设置如图 4-14 所示。

在【例外】选项卡中,可以启用或禁用一个现有的程序或服务,或者维护用于定义例外通信的程序和服务列表。在【常规】选项卡中选定【不允许例外】复选框后,例外通信将不被允许。

(1) 添加程序:单击【添加程序】按钮,显示【添加程序】对话框,可以从中选择一个程序或者浏览查找一个程序文件名,如图 4-15 所示。

(2) 添加端口:单击【添加端口】按钮,显示【添加端口】对话框,可以从中配置 TCP 或 UDP 端口,如图 4-16 所示。

Windows 防火墙允许指定例外通信的范围,这个范围定义了哪一部分的网络连接产生的例外通信是被允许的。要定义一个程序或端口的范围,应单击【更改范围】按钮,打开的对话框如图 4-17 所示。

在定义一个程序或端口的范围时,有三个选项可以选择:

① 任意计算机(包括 Internet 上的计算机)。从任何 IPv4 地址发出的例外通信都是被允许的。这种设置可能会使计算机容易受到 Internet 上的恶意用户或程序的攻击。

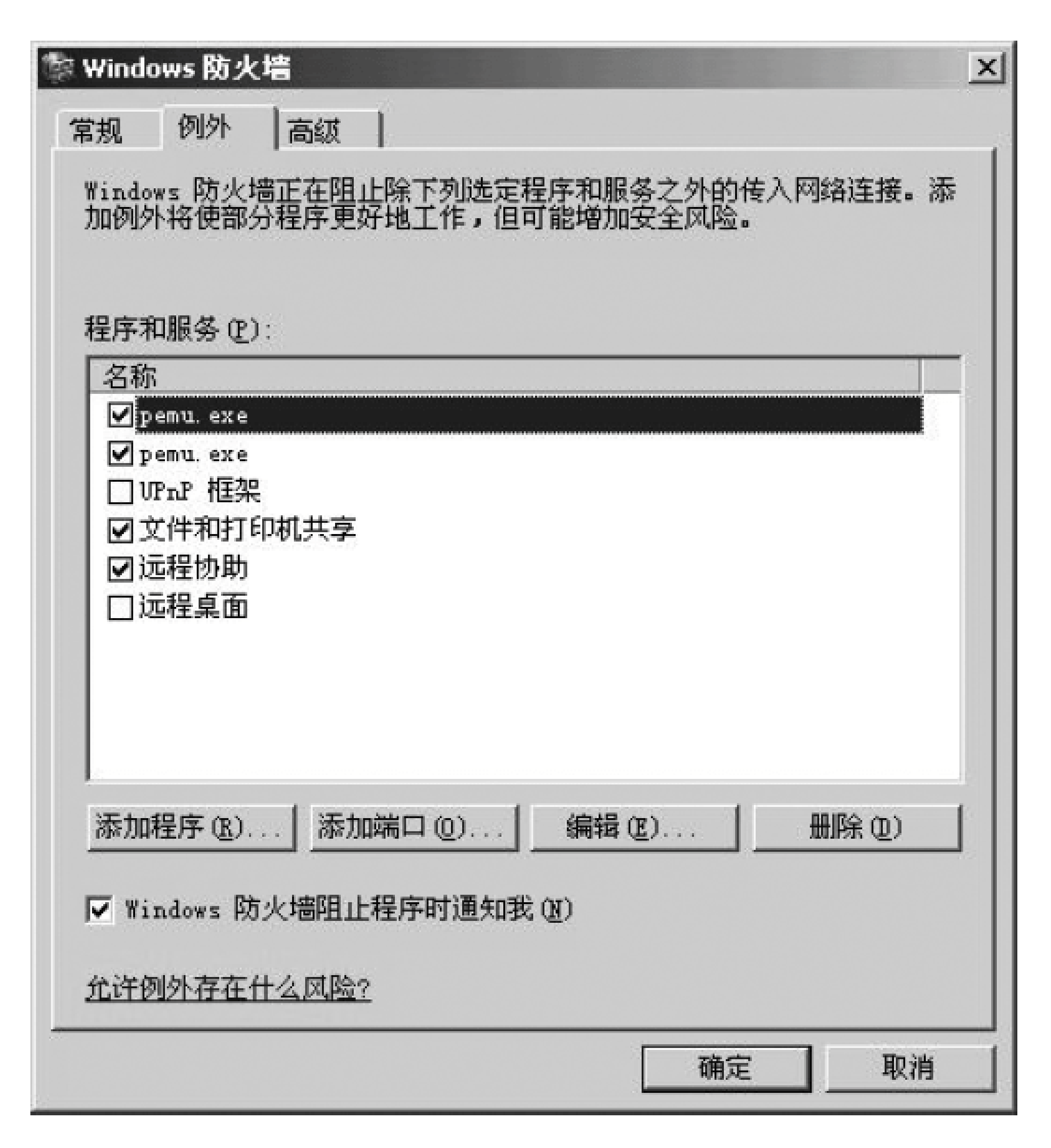


图 4-14　【例外】选项卡



图 4-15　【添加程序】对话框

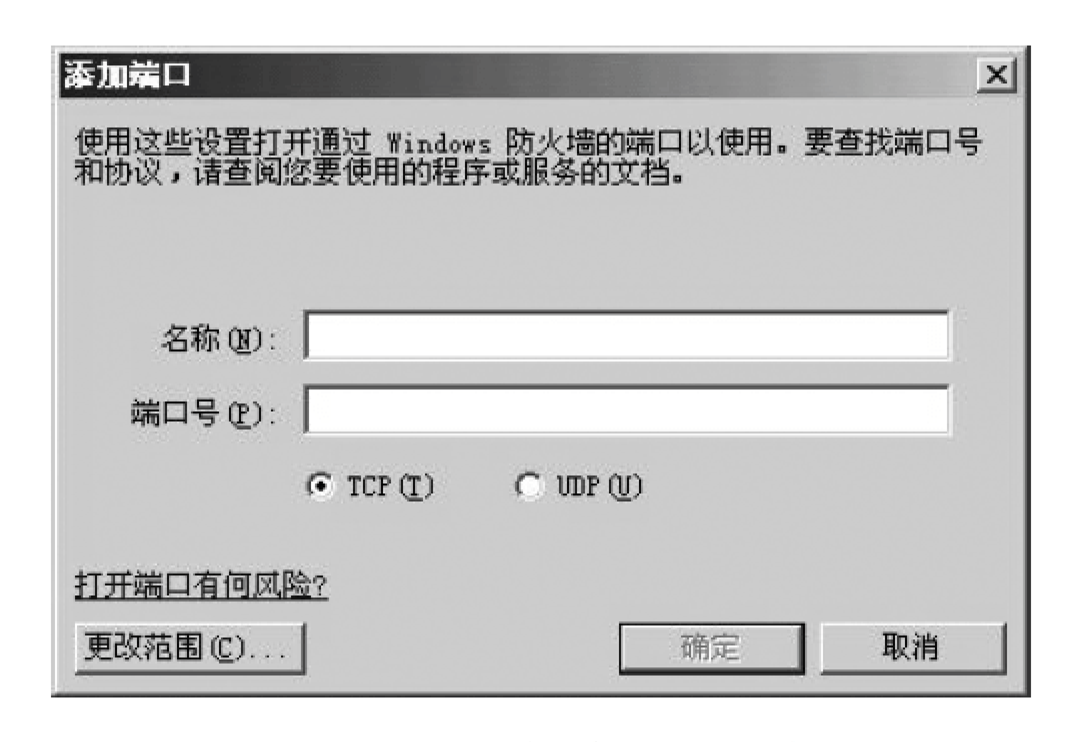


图 4-16　【添加端口】对话框

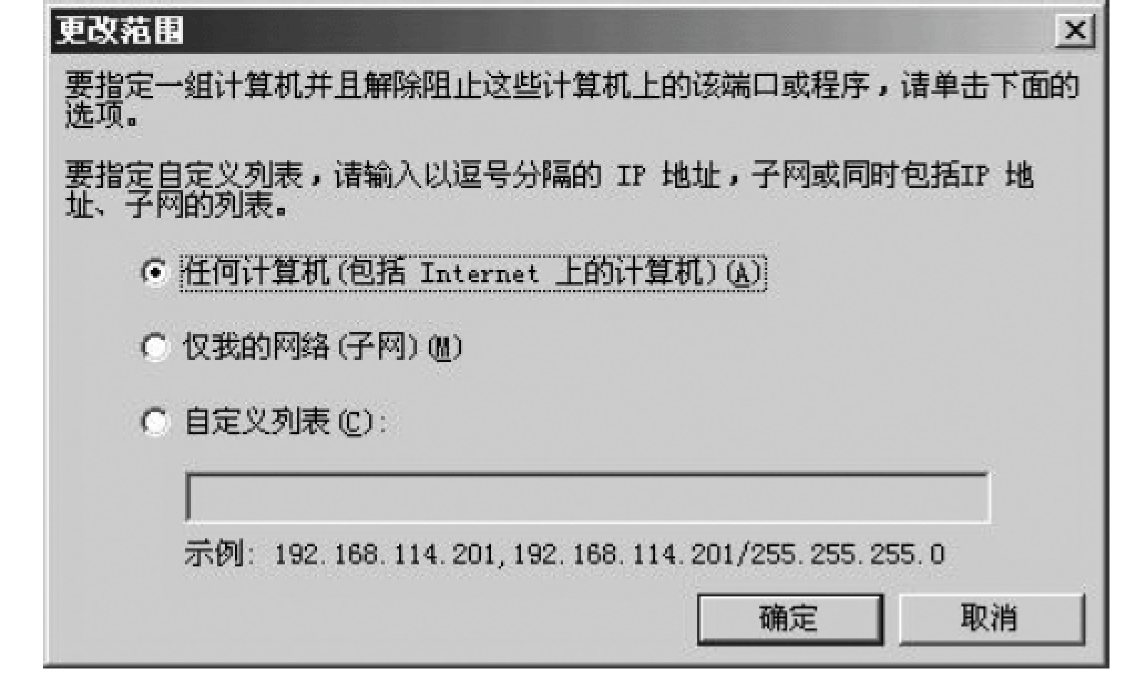


图 4-17　【更改范围】对话框

② 仅我的网络(子网)。只有从符合以下条件的 IPv4 地址发出的例外通信才是被允许的，即与接收通信的网络连接所连的本地网络段(子网)相匹配的 IPv4 地址被允许。比如，如果网络连接所配置的 IPv4 地址是 192.168.12.101，并带有子网掩码 255.255.0.0，那么只有从 192.168.0.1 到 192.168.255.254 的 IPv4 地址发出的例外通信才是被允许的。

③ 自定义列表。可以指定一个或多个用逗号分割的 IPv4 地址或 IPv4 地址范围。IPv4 地址范围通常对应于子网。对 IPv4 地址来说，用点分十进制记法键入 IPv4 地址。对 IPv4 地址范围来说，可以使用点分十进制子网掩码或前缀长度来指定一个范围。当使用点分十进制子网掩码时，可以把范围指定为一个 IPv4 网络 ID(如 10.10.4.0/255.255.255.0)或者使用一个在范围内的 IPv4 地址(如 172.16.10.11/255.255.255.0)来指定范围。当使用网络前缀长度时，可以将范围指定为一个 IPv4 网络 ID(如 172.16.31.0/24)或者使用一个在范围内的 IPv4 地址(如 10.10.5.10/24)来指定范围。下面是自定义列表的一个示例：

192.168.2.102,10.10.4.0/255.255.255.0,172.16.31.0/24,172.16.10.11/255.255.255.0



在只允许本地网络中的计算机(它们都连接在同一个子网中)访问一个程序或服务,而不允许潜在的恶意 Internet 用户访问时,"仅我的网络(子网)"范围会很有用。

程序或端口一旦被添加,它就在【程序和服务】列表中被默认禁用。

对于在【高级】选项卡中选定的所有连接,所有在【例外】选项卡中启用的程序和服务都将启用。

3)【高级】选项卡

【高级】选项卡包括下面几个部分,图 4-18 显示了【高级】选项卡。



图 4-18 【高级】选项卡

(1) 网络连接设置。在【网络连接设置】选项区中,可以指定一组用于启用 Windows 防火墙的接口。如要启用,应选中网络连接名称旁边的复选框。如要禁用,应取消选中该复选框。默认情况下,所有的网络连接都启用了 Windows 防火墙。如果某个网络连接没有出现在此列表中,那么它就不是一个标准网络连接。这方面的例子包括一些 Internet 服务提供商(ISP)提供的自定义拨号程序。

单击一个网络连接的名称,然后单击【设置】按钮,即可以配置这个网络连接的高级设置。

如果清除了【网络连接设置】选项区中的所有复选框,Windows 防火墙将不再保护计算机,不管是否已经在【常规】选项卡中选择了【启用(推荐)】单选按钮都是如此。如果在【常规】选项卡中选择了【不允许例外】复选框,【网络连接设置】选项区中的设置就会被忽略,在这种情况下所有的接口都将被保护。

单击【设置】按钮,【高级设置】对话框即会显示,如图 4-19 所示。

在【高级设置】对话框中,可以在【服务】选项卡中(仅通过 TCP 或 UDP 端口)配置特定的服务,或者在 ICMP 选项卡中启用特定的 ICMP 通信类型。





（2）安全日志。在【安全日志记录】选项区中，单击【设置】按钮，在打开的【日志设置】对话框中指定 Windows 防火墙日志的配置，如图 4-20 所示。



图 4-19 网络连接的【高级设置】对话框



图 4-20 【日志设置】对话框

在【日志设置】对话框中，可以配置是否记录丢弃的数据包和成功的连接，并且指定日志文件（默认设置为 Systemroot\pfirewall.log）的名称和位置及其最大的数据量。

（3）ICMP。在【ICMP】选项区中，可以单击【设置】按钮来指定在【ICMP 设置】对话框中允许的 ICMP 通信类型，如图 4-21 所示。

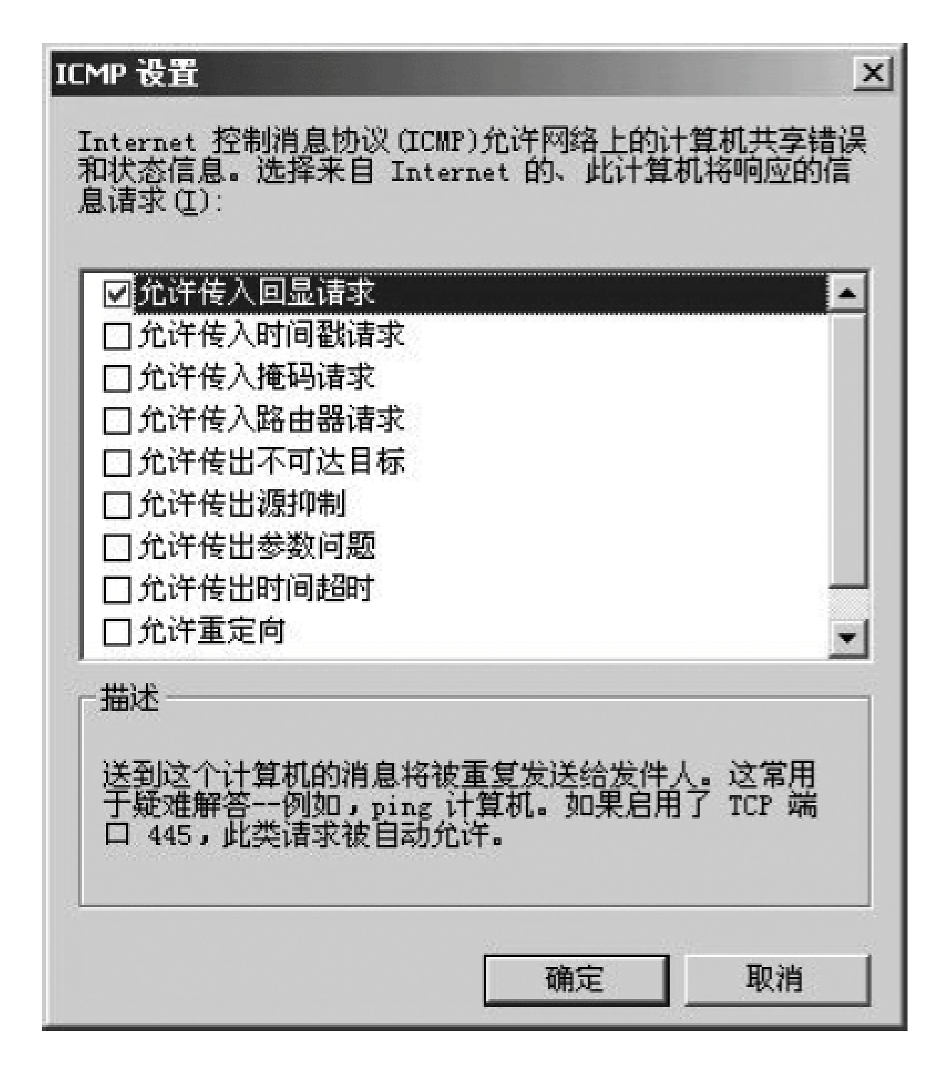


图 4-21 【ICMP 设置】对话框

在【ICMP 设置】对话框中，可以启用或禁用传入 ICMP 消息的类型，Windows 防火墙允许所有在【高级】选项卡中选定的连接使用这些消息。ICMP 消息被用来进行诊断、报告错误条件和进行配置。默认情况下，列表中的任何 ICMP 消息都不被允许。

解决连接问题的一个常用方法就是使用 ping 工具来测试试图连接的计算机的地址。在用 ping 命令时，发送一个 ICMP Echo 消息后会收到一个 ICMP Echo Reply 消息。默认情况下，Windows 防火墙不允许传入 ICMP Echo 消息，因此计算机就不能回送一个 ICMP Echo Reply。要配置 Windows 防火墙以使其允许传入 ICMP Echo 消息，必须选中【允许传入回显请求】复选框。

（4）默认设置。单击【恢复默认值】按钮，将 Windows 防火墙重置为它的原始安装状态。

2．关闭 Windows 防火墙

在如图 4-13 所示的【Windows 防火墙】对话框中选择【关闭（不推荐）】单选按钮，单击【确定】按钮即可。



4.7.2 Windows 防火墙的应用

1. 让 Windows XP SP2 正确识别 UPnP(通用即插即用)

BitComet 以其拥有内网互联(NAT Traversal)技术,而且支持 UPnP 的 NAT 和 Windows XP 防火墙,让内网的朋友在进行 BT 下载时可以获得相当快的下载速度。但自从升级到 SP2 并启用了 Windows 防火墙后,BitComet 软件速度变得很慢!这是由于防火墙没有设置好,使得系统没能正确识别 UPnP 设备。

(1) Windows XP 默认是支持 UPnP 的,如果在【例外】选项卡中看不到这个选项,则说明没有安装 UPnP 设备支持。打开【网上邻居】窗口,在其左侧的列表中单击【显示联网的 UPnP 设备的图标】超链接,如果 UPnP 设备文件没有安装或安装不正确,系统就会自动安装,如图 4-22 所示。

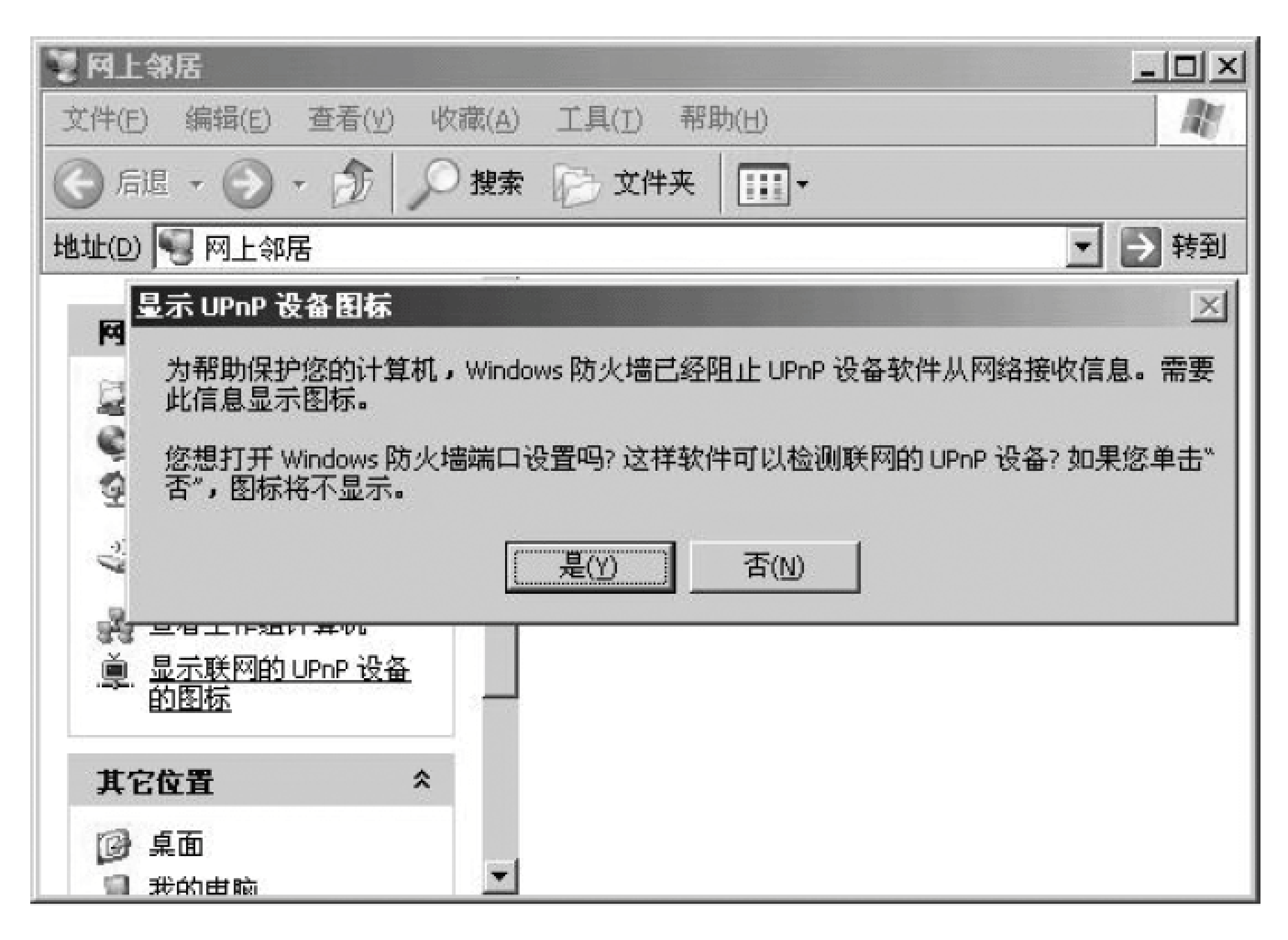


图 4-22 显示联网的 UPnP 设备的图标

(2) 打开防火墙配置窗口并启动防火墙,确认没选中【不允许例外】选项;当打开 BitComet 后,Windows 防火墙有可能会提示用户是否要阻止该程序,选择【解除阻止】选项。

(3) 选择【例外】选项卡,选中【UPnP 框架】复选框即可。

2. 给远程管理开个通行证

当通过 MMC(Microsoft Management Console,微软管理控制台)中的计算机管理、磁盘管理等组件远程管理程序来管理局域网上的其他计算机时,计算机必须开放 TCP 445 端口。如果在远程操作已经安装 Windows XP 并开启了防火墙的计算机时,就得手动打开这个 TCP 端口,方法如下:

(1) 打开【Windows 防火墙】窗口,切换到【例外】选项卡,选中【文件和打印机共享】复选框。

(2) 单击【编辑】按钮,在打开的【编辑服务】窗口中选中【TCP 445】复选框,单击【更改范围】按钮,选中【仅我的网络(子网)】单选按钮或者选中【自定义列表】单选按钮并输入要控



制的计算机的 IP 地址，如图 4-23 所示。

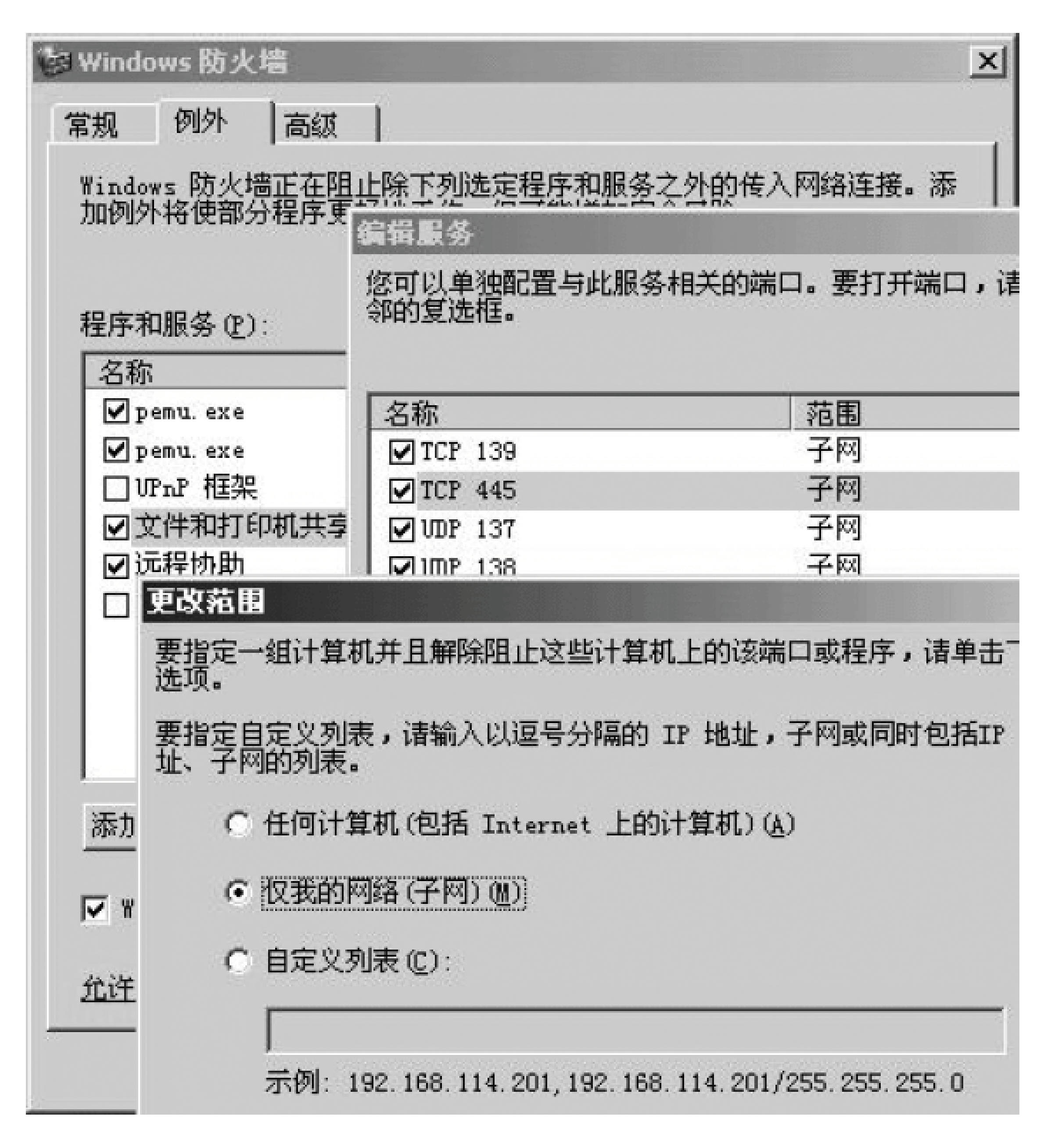


图 4-23　开放 TCP 445 端口

3. "远程桌面"连接

通过 Windows XP 防火墙实现远程协助的方法很简单。远程协助使用的是动态端口。在【Windows 防火墙】对话框中的【例外】选项卡上的【程序和服务】列表框中选择【远程协助】复选项，这样 Windows 将自动监视并正确处理来自 sessmgr.exe 应用程序的所有通信请求并完成连接。Windows NetMeeting 的远程桌面要复杂一些，尽管在【例外】选项卡中有【远程桌面】选项，但是如果选择这个选项，实际是开放了 TCP 的 3389 端口，因此可能无法完成远程桌面连接。

在 Windows 防火墙打开的情况下，在可以使用 Windows NetMeeting 的远程桌面共享功能之前，必须向 Windows 防火墙的【例外】选项卡上【程序和服务】列表框中分别为%systemroot%\System32\Mnmsrvc.exe 文件和 C:\ProgramFiles\NetMeeting\conf.exe 文件添加程序，如图 4-24 所示。

4. 只让内网用 ping 命令连接本机

在默认情况下，Windows XP 防火墙不允许 ICMP 入站数据进入，也就不会回复 ICMP 返回的数据，这样可以防止用户使用检查网络故障常用的命令工具"Ping"来探测计算机。不过这样对于一些启用了共享上网的用户，内网也无法用 ping 命令来检查本地网络情况了。解决方法如下：

方法一：按照前述的方法，分别使【文件和打印机共享】中所打开的 TCP 端口适用于子网即可。



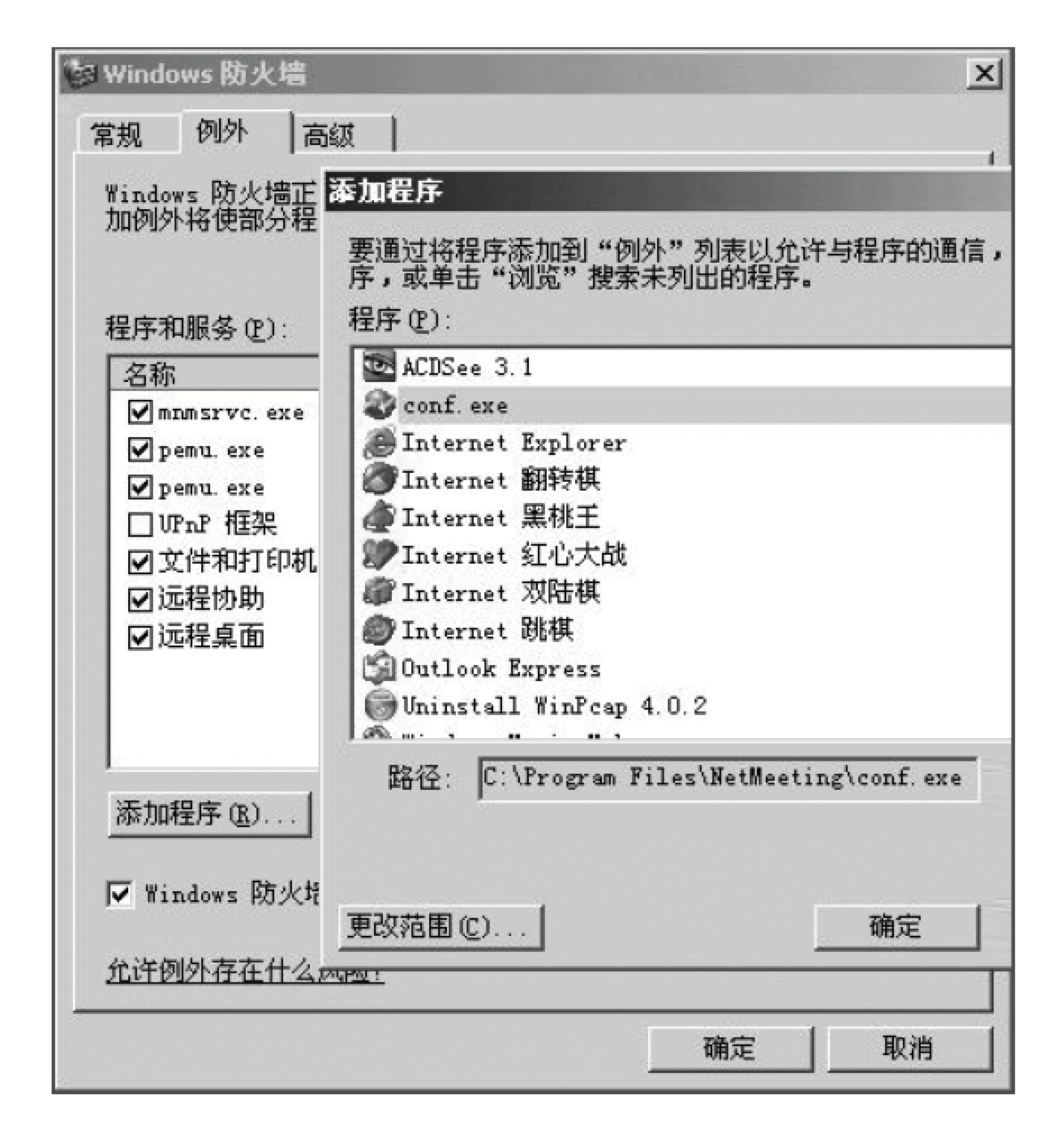


图 4-24　NetMeeting 远程桌面的设置

方法二：打开【Windows 防火墙】对话框，切换到【高级】选项卡，双击与内网连接的【本地连接】复选框，再切换到【ICMP 设置】对话框，选中【允许传入回显请求】复选框，然后确认所有操作。

提示：ICMP(Internet Control Message Protocol，Internet 控制消息协议)是 TCP/IP 协议簇中的一个子协议，用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息，这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。在网络中经常会使用到 ICMP 协议，只不过我们觉察不到而已。比如我们经常使用的用于检查网络通不通的 ping 命令实际上就是 ICMP 协议工作的过程，还有诸如跟踪路由的 tracert 命令也是基于 ICMP 协议的。

4.8　习　　题

1. 简述防火墙的主要功能。
2. 简述防火墙的分类。
3. 对比各类防火墙的特点。
4. 简述防火墙采用的主要技术，比较它们的优缺点。
5. 简述防火墙有哪几种体系结构。
6. 防火墙配置的基本原则是什么？
7. 简述用户在选择防火墙时考虑的主要因素。
8. 简述如何使用 Windows 防火墙关闭或打开端口，举例说明。



第5章　ISA Server 2006 的应用配置

本章学习目标：

- ISA Server 2006 的主要功能。
- ISA Server 2006 的安装。
- ISA Server 2006 的网页缓存。
- ISA Server 2006 的客户端应用。
- ISA Server 2006 在网络保护方面的配置。

ISA(Internet Security and Acceleration，Internet 安全和加速)Server 是微软公司推出的一款网关型安全产品，是一款优秀的软件防火墙。ISA Server 具备防火墙、应用层防护、VPN 与网页缓存等优异功能，是企业网络安全防护的绝佳选择。自从在 2000 年推出 ISA Server 2000 版本以来，特别受用户欢迎，在中、小型企业中得到了广泛应用。ISA Server 2006 是 ISA Server 的最新版本。

5.1　ISA Server 简介

ISA Server 是建立在 Windows Server 2003 操作系统上的一种可扩展的企业级防火墙和 Web 缓存服务器。ISA Server 的多层防火墙可以保护网络资源免受病毒、黑客的入侵和未经授权的访问。而且，通过本地而不是 Internet 为对象提供服务，其 Web 缓存服务器允许组织能够为用户提供更快的 Web 访问。在网络内安装 ISA Server 时，可以将其配置成防火墙，也可以配置成 Web 缓存服务器，或两者兼备。

5.1.1　ISA Server 2006 的主要功能

ISA Server 2006 是一款优秀的符合现代企业需求的多功能产品，其优异的功能主要表现在以下几个方面。

1. 防火墙(Firewall)

ISA Server 2006 可以安装成专用防火墙，控制内部网络与 Internet 之间的通信，增强网络的安全性。还可以利用它安全地发布企业内部的服务器(例如网站、电子邮件服务器



等)，以便让客户与合作伙伴来分享内部网络的资源。

作为防火墙，ISA Server 2006 允许设置一组广泛的规则，以指定能够通过 ISA Server 2006 的站点、协议和内容，由此实现商业 Internet 安全策略。通过监视内部客户端和 Internet 之间的请求和响应，ISA Server 2006 可以控制哪些人能够访问公司网络里的哪台计算机。ISA Server 2006 还能控制内部客户端能够访问 Internet 上的哪台计算机。

2. 虚拟专用网(VPN)

虚拟专用网(VPN)可以让远程用户与局域网(LAN)之间，或者是分别位于两地的局域网之间，通过 Internet 来建立一个安全的通道。

3. Web 缓存服务器

通过将用户经常访问的网页保存到 ISA Server 2006 的硬盘与内存(RAM)，不但让用户更快地访问到所需的网页，同时也可以提高网络的效率，节省网络的带宽。

5.1.2 多网络结构

ISA Server 支持多网络结构，例如 ISA Server 同时连接总公司网络、分公司网络、DMZ 网络、外地 VPN 客户端网络与外部网络(Internet)，如图 5-1 所示。

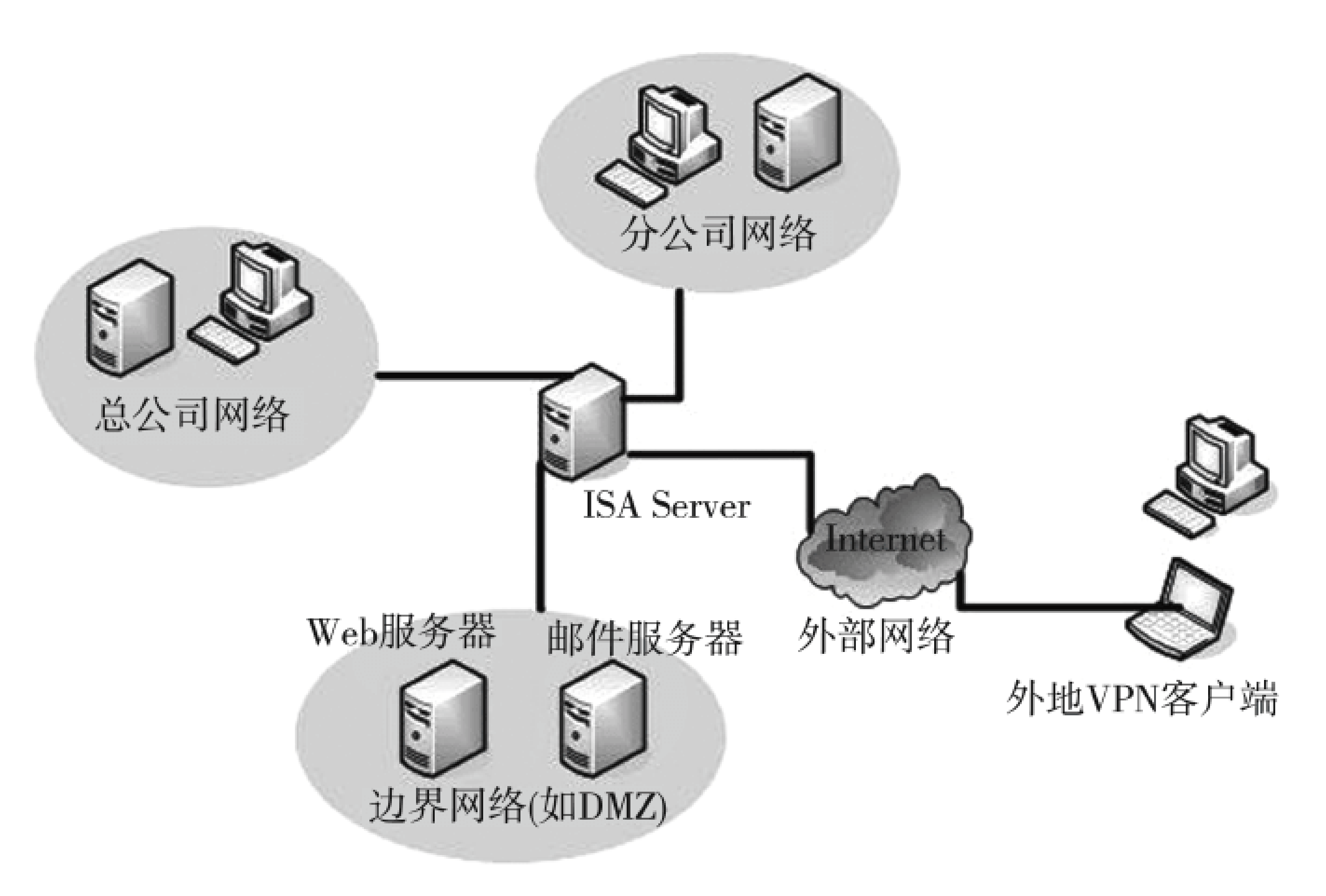


图 5-1　ISA 多网络结构示例

在这种多网络(网络集)结构中，可以通过 ISA Server 防火墙来设置在任意两个网络之间的连接规则，从而允许网络之间相互访问。这种连接规则在 ISA Server 中称为网络规则。

5.1.3 防火墙的设置种类和网络模板

ISA Server 包含与常见网络拓扑对应的网络模板，每种网络模板对应一种防火墙的设置种类，ISA Server 会自动根据用户当前的网络环境和配置选择一种默认的模板。ISA



Server 的网络模板主要分为边缘防火墙、3 向外围网络防火墙、前端防火墙、后端防火墙和单一网络适配器五种。这些网络模板提供了一些默认策略，通过应用模板将 ISA Server 配置为某种防火墙时，ISA Server 将按照所选模板的默认策略配置网络规则和防火墙策略。

1. 边缘防火墙

如图 5-2 所示为边缘防火墙的架构，其中的 ISA Server 防火墙计算机有两个网络接口(例如两片网卡)，一个网络接口连接到内部网络，另一个连接到外部网络(Internet)。也就是说防火墙介于内部网络与 Internet 之间。这种架构能够保护内部网络的安全，避免外来入侵者访问内部网络资源。也可以开放让内部用户来访问外部资源，这是最容易架设的防火墙架构。

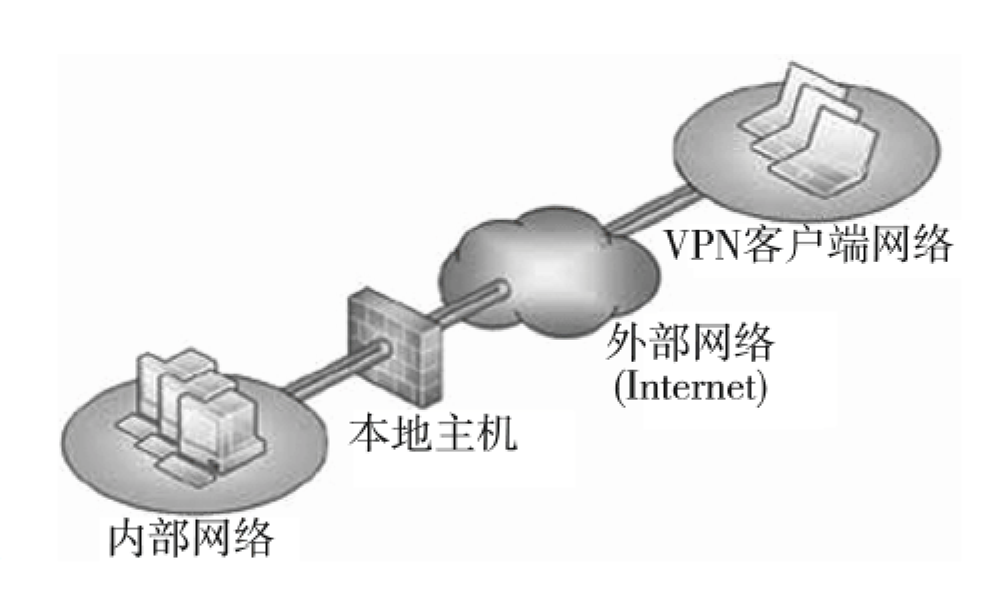


图 5-2　边缘防火墙

如果想保护网络不会被他人访问，同时允许公司网络上的用户进行特定的访问，可以将 ISA Server 设置作为边缘防火墙。

2. 三向外围网络防火墙

如图 5-3 所示，这种方案涉及设置具备 3 个网络适配器的 ISA Server：一个网络适配器连接到 Internet(外部网络)，另一个连接到内部网络，第三个连接到外围网络。这是一种非常典型的网络配置方案，三向外围网络模板适用于这种方案。此模板采用 ISA Server 连接到内部网络、外部网络和外围网络(也称 DMZ、网络隔离或被筛选的子网)的网络拓扑。

3. 前端防火墙

如图 5-4 所示，这种方案涉及在网络的边缘部署 ISA Server，其中在后端配置另一个防火墙，用于保护内部网络。在这个方案中，ISA Server 作为背靠背外围网络配置中的防御前线。前端网络模板适用于这个方案。此模板采用 ISA Server 在网络边缘，另一个防火墙配置在后端(保护内部网络)的网络拓扑。

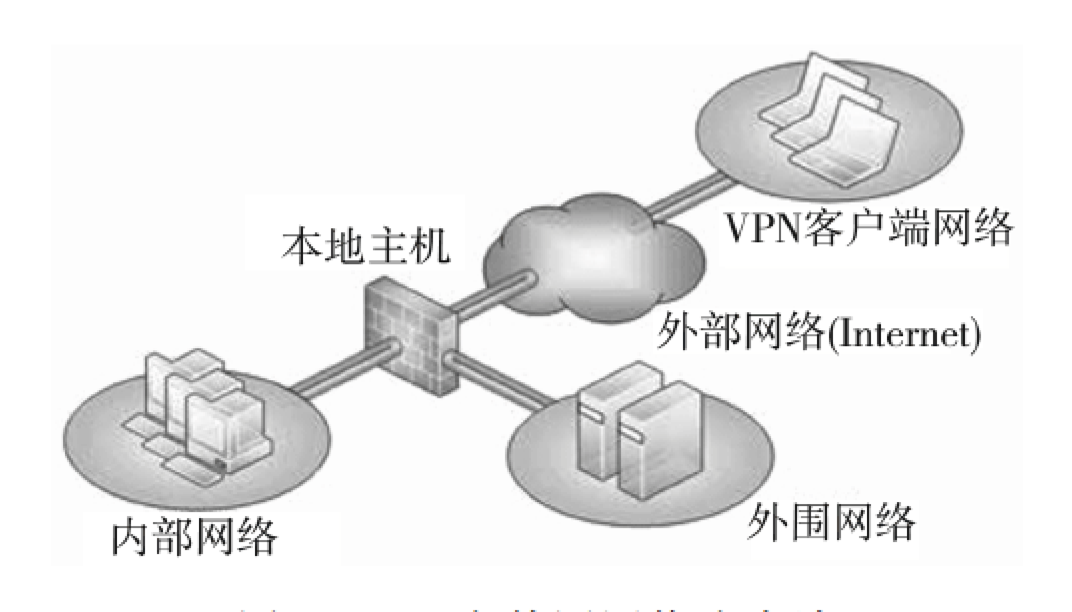


图 5-3　三向外围网络防火墙

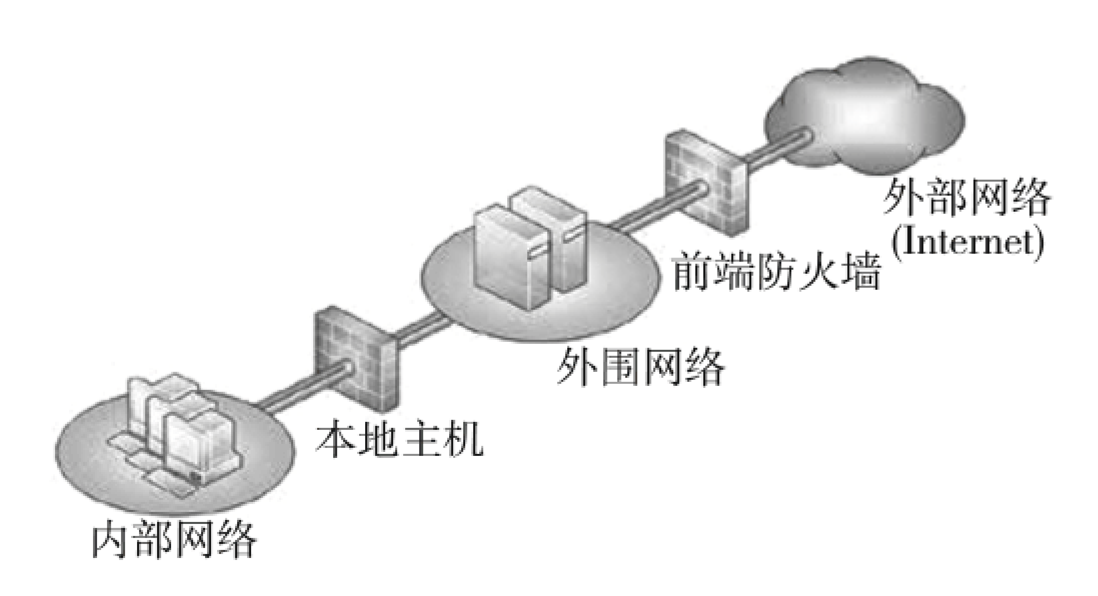


图 5-4　前端防火墙

4. 后端防火墙

如图 5-5 所示，这种方案涉及在外围网络和内部网络之间部署 ISA Server，其中在后端



配置另一个防火墙，用于保护内部网络。在这个方案中，ISA Server 作为背靠背外围网络配置中的后防线，后端网络模板适用于这个方案。此模板采用 ISA Server 部署在外围网络和内部网络之间，另一个防火墙配置在后端(保护内部网络)的网络拓扑。

5. 单一网络适配器

如图 5-6 所示，可以在具有单一网络适配器的计算机上安装 ISA Server。通常，当另一防火墙位于网络的边缘时进行此安装，以便将公司资源连接到 Internet。在此单一适配器方案中，ISA Server 通常作为缓存服务器，对 Internet 中的内容进行缓存，供公司网络中的客户端使用。此模板采用在外围或公司网络内部配置一个单一网络适配器的方法。在这种配置中，ISA Server 用作 Web 代理和缓存服务器。

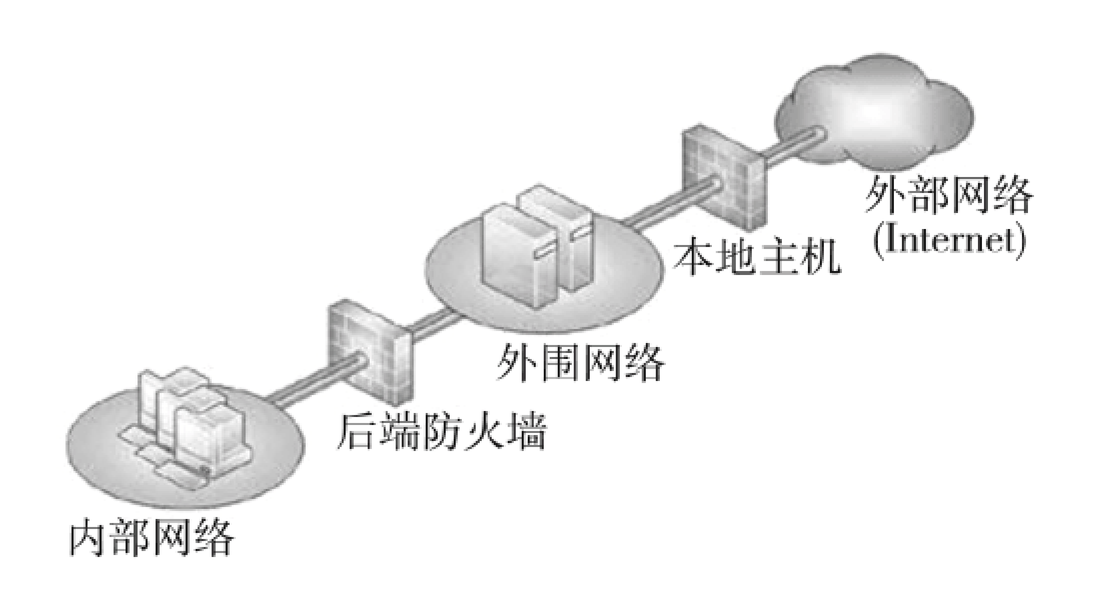


图 5-5　后端防火墙

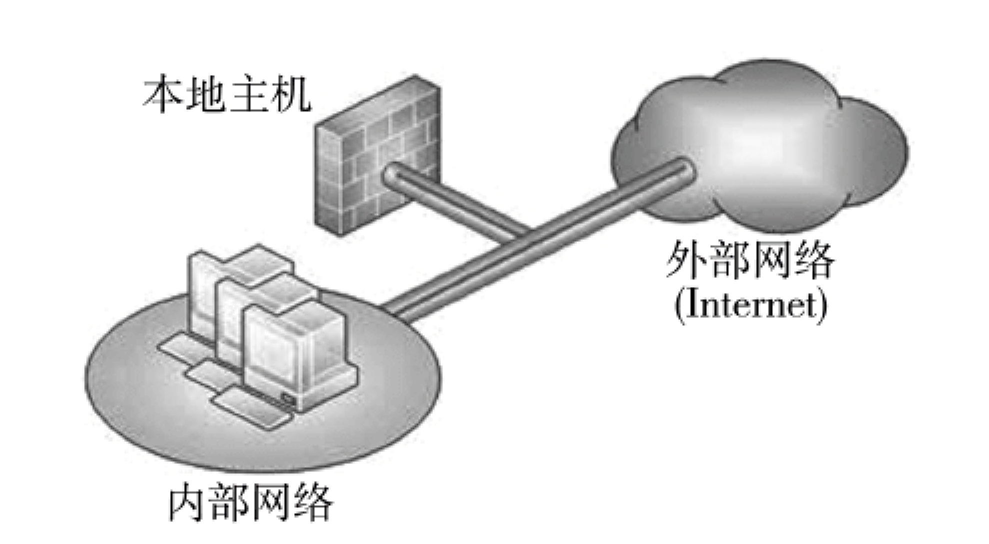


图 5-6　单一网络适配器

5.1.4　ISA Server 与 VPN 的集成

很多企业利用 Internet 将位于各地的局域网连接起来，但是必须确保网络之间所传送数据是安全的。而虚拟专用网(Virtual Private Network，VPN)就是提供此功能的技术，它让局域网之间可以通过 Internet 来建立一个安全的通道。

5.1.5　ISA Server 缓存的种类

在网页缓存服务器中又分为“正向网页缓存服务器”和“反向网页缓存服务器”，ISA Server 2006 都可以做到。

作为正向网页缓存服务器，ISA Server 2006 保存集中缓存内经常受到请求的 Internet 内容，专用网络内的任何 Web 浏览器都可以访问这些内容，这样可以改善客户端浏览器的性能，缩短响应时间，并且减少 Internet 连接的带宽消耗。

作为反向网页缓存服务器，ISA Server 2006 用缓存中的 Web 内容来满足传入的客户端请求。只有缓存中的内容不能满足请求时，它才会把请求转发给 Web 服务器。

5.1.6　ISA Server 与其他软件防火墙的比较

相对于其他类型软件防火墙解决方案，ISA Server 的主要优势包括了它的高级应用层



检测和保护功能，易于使用，并提供快速、安全的 Internet 访问的能力，分布式防火墙集中管理能力，以及易于与目前的防火墙和 VPN 结构集成的功能。具体优势体现在以下几个方面。

1. 高级保护

ISA Server 旨在通过提供有状态数据包过滤和链路过滤来保护企业免遭新型的攻击。状态数据包过滤确定允许哪些数据包受保护的网络链路和应用程序层代理服务。

状态过滤动态打开所需要的端口，并在通信结束时关闭这些端口。链路过滤为 Microsoft Windows Media 技术、Telnet、RealAudio、IRC 以及许多其他 Internet 协议和服务的多平台访问提供了应用层透明的链路网关。ISA Server 的链路层安全性与动态数据包过滤配合工作，从而增强了安全性和易用性。

除了状态数据包和链路过滤以外，ISA Server 还使用应用程序、命令和数据感知过滤器控制应用程序特定通信。通过对 VPN、HTTP、文件传输协议(FTP)、简单邮件传输协议(SMTP)、邮局协议版本 3（POP3)、域名系统(DNS)、H. 323 会议、流媒体和远程过程调用(RPC)通信进行智能过滤，ISA Server 可以根据通信的内容来接受、拒绝、重定向和修改通信。

2. 易于使用

ISA Server 十分灵活，并易于管理员使用。它包含了多重网络体系结构功能，集成的 VPN，以及通过强健的虚拟策略编辑器，节省时间的网络模板，自动化的防火墙策略向导，以及增强的故障解决工具，实现对防火墙的直观管理。

ISA Server 还可以通过自动安装防火墙和 Web 缓存服务来简化防火墙安装。此外，ISA Server 标准版支持输出本地防火墙策略，并且 ISA Server 企业版还支持将本地防火墙策略和配置信息导出到(XML)文件，对每个阵列的防火墙成员、防火墙用户组以及更多内容进行实时的防火墙会话监控。

3. 快速、安全的访问

ISA Server 通过将 VPN 功能完全集成到防火墙体系结构，加速 Web 缓存和优化防火墙过滤引擎，提供了快速、安全的 Internet 访问。用于站点到站点 VPN 连接的内置 IPSec 隧道模式支持，使连接 ISA Server 与分支机构 VPN 网关变得十分容易。IPSec 隧道模式与第三方 VPN 网关的连接，包括了深入的 VPN 客户端检查和防火墙策略支持，有助于企业建立更安全的虚拟专用网络和防火墙基础架构。对最新的第三方过滤器和综合软件开发工具包(SDK)的支持进一步扩展了 ISA Server 的功能。

4. 集中日志和报告

ISA Server 标准版可以记录所有通过防火墙的活动，而企业版则允许集中记录和报告所有企业成员的活动。集中化的日志和报告极大地简化了搜寻基于每个用户、组、服务器、网络信息的工作。ISA Server 包括一个综合报告生成器，它记录了通过任意 ISA Server 而产生的关于 Internet 活动的主要信息。



5. 与现有防火墙和 VPN 构架轻松集成

很多公司想要利用 ISA Server 应用层检测能力能提供的那种增强的安全级别，但是他们已经有了一个防火墙和 VPN 构架，同时不想或者不需要重新构建一个新的构架。ISA Server 支持这些企业将其强大功能与现有的防火墙和 VPN 构架轻松地结合。

一个或多个 ISA Server 计算机可以放置在状态包检测防火墙后面工作，以最少的管理费增强整个企业的安全性。ISA Server 计算机也可以放置在特定用户、部门和服务区域前面工作，从而提供增强的状态过滤和对这个网段进行状态应用层检测。

5.2 利用 VMware Workstation 建立测试环境

5.2.1 VMware Workstation 概述

VMware Workstation 允许操作系统和应用程序在一台虚拟机内部运行。虚拟机是独立运行主机操作系统的离散环境。在 VMware Workstation 中，可以在一个窗口中加载一台虚拟机，它可以运行自己的操作系统和应用程序。可以在运行于桌面上的多台虚拟机之间切换，通过一个网络共享虚拟机(例如一个公司局域网)，挂起和恢复虚拟机以及退出虚拟机，这一切不会影响用户的主机操作和任何操作系统或者它正在运行的应用程序。

VMware Workstation 是一款功能强大的桌面虚拟计算机软件，提供用户可在单一的桌面上同时运行不同的操作系统，和进行开发、测试、部署新的应用程序的最佳解决方案。VMware Workstation 可在一部实体机器上模拟完整的网络环境，以及可便于携带的虚拟机器，其更好的灵活性与先进的技术胜过了市面上其他的虚拟计算机软件。对于企业的 IT 开发人员和系统管理员而言，VMware 在虚拟网路、实时快照、拖曳共享文件夹、支持 PXE 等方面的特点使它成为必不可少的工具。

5.2.2 搭建 ISA Server 2006 测试环境的步骤

1. 安装 VMware Workstation

从 VMware 官方网站 www.vmware.com(或提供共享软件下载的网站，如天空软件站 www.skycn.com)下载 VMware Workstation，同时注册以便取得试用序列号，然后将其安装到 Windows Server 2003(建议采用 Windows Server 2003 R2 EnterPrise Edition)的计算机上。

(1) VMware Workstation 内建了 10 个虚拟网络。

① VMnet0(default bridged)：是真实网卡连接的网络，也就是外部网络，本书后面的实验中 ISA Server 的外网卡就是连接在这个网络上。

② VMnet1(Host-only)：连接着内部网络，本书之后实验中 ISA Server 的内网卡就是连接在这个网络上。

③ VMnet2～VMnet7 与 VMnet9：可以利用它们建立 DMZ 网络。

④ VMnet8(NAT)：它提供 NAT(Network Address Translation，网络地址转换)功能。

（2）VMware Workstation 安装完成后，这台计算机内除了原有的网卡（名称为“本地连接”）外，还会另外自动新建两张虚拟网卡，如图 5-7 所示。



图 5-7　添加了两张虚拟网卡

图中的三张网卡的说明如下。

① 本地连接：它是安装在这台计算机上的物理网卡，如果想让这台计算机可以正常上网，可以根据网络环境设置正确的 TCP/IP 配置。

② VMware Network Adapter VMnet1：它是连接到 VMnet1 的虚拟网卡，如果想让这台计算机可以跟内部网络的其他虚拟计算机沟通，应将 IP 地址改为与内部计算机在同一网段（即相同的网络号），如图 5-8 所示。

③ VMware Network Adapter VMnet8：它是连接到 VMnet8 的虚拟网卡。

2. 建立含 Windows Server 2003 的虚拟机

利用 VMware Workstation 建立一个虚拟机，并在此机器内安装 Windows Server 2003 操作系统，但在后面的实验中不在这套系统内安装 ISA Server 2006，也不会使用此系统，而是将这套系统的虚拟硬盘作为母盘，之后如果需要更多 Windows Server 2003 虚拟机时，只要克隆（Clone）这套系统即可，不需要从头开始安装，如此可以节约大量的时间。方法如下：

（1）选择【开始】/【所有程序】/VMware/VMware Workstation 命令，启动 VMware Workstation。

（2）在【起始页】上，单击【新建虚拟机】图标，如图 5-9 所示。

（3）在【新建虚拟机向导】对话框中单击【下一步】按钮。

（4）选择【典型】单选按钮，单击【下一步】按钮。然后在【版本】下拉列表中选择 Windows Server 2003 Enterprise Edition，如图 5-10 所示，单击【下一步】按钮。

（5）为此虚拟机命名。在此，将这套要当作母系统（Master）的虚拟机取名为 2003Master，它的相关文件默认是放在【我的文档】中的 My Virtual Machines 文件夹中，可以改变存放的位置，如改为 E:\VMware 文件夹。完成后单击【下一步】按钮，如图 5-11 所示。



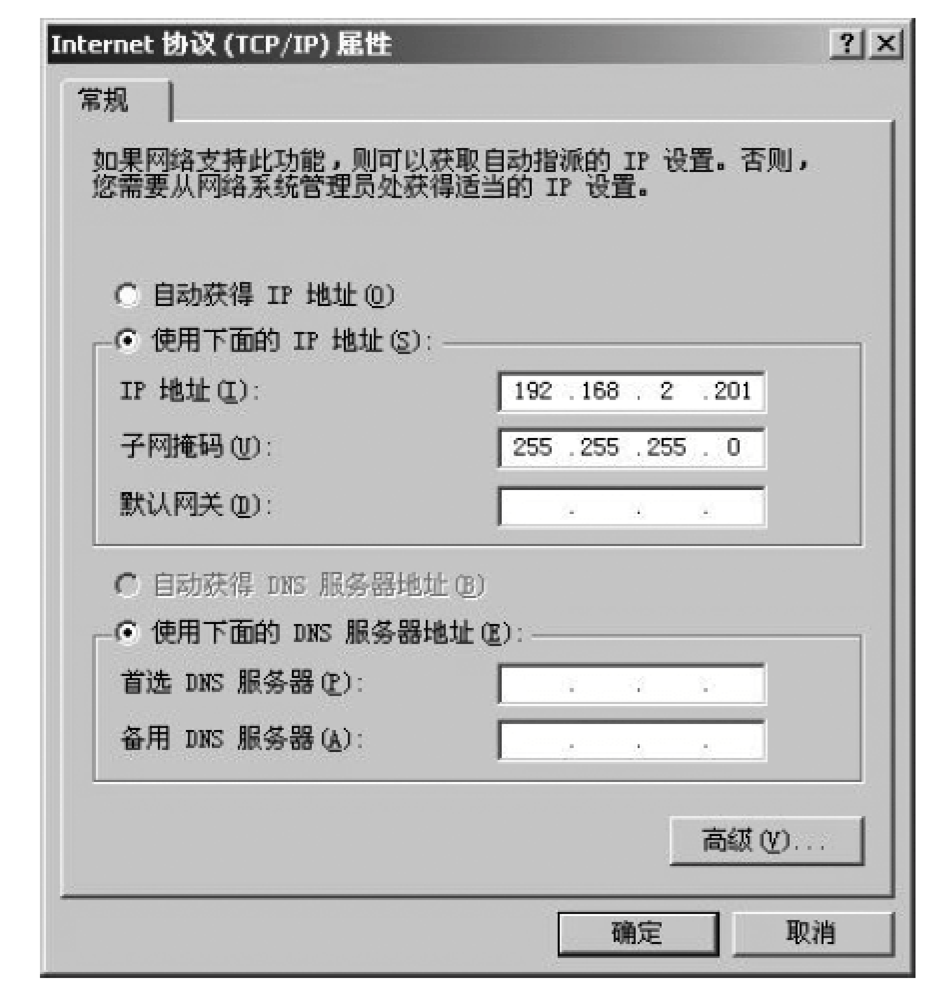


图 5-8　VMnet1 的虚拟网卡的设置

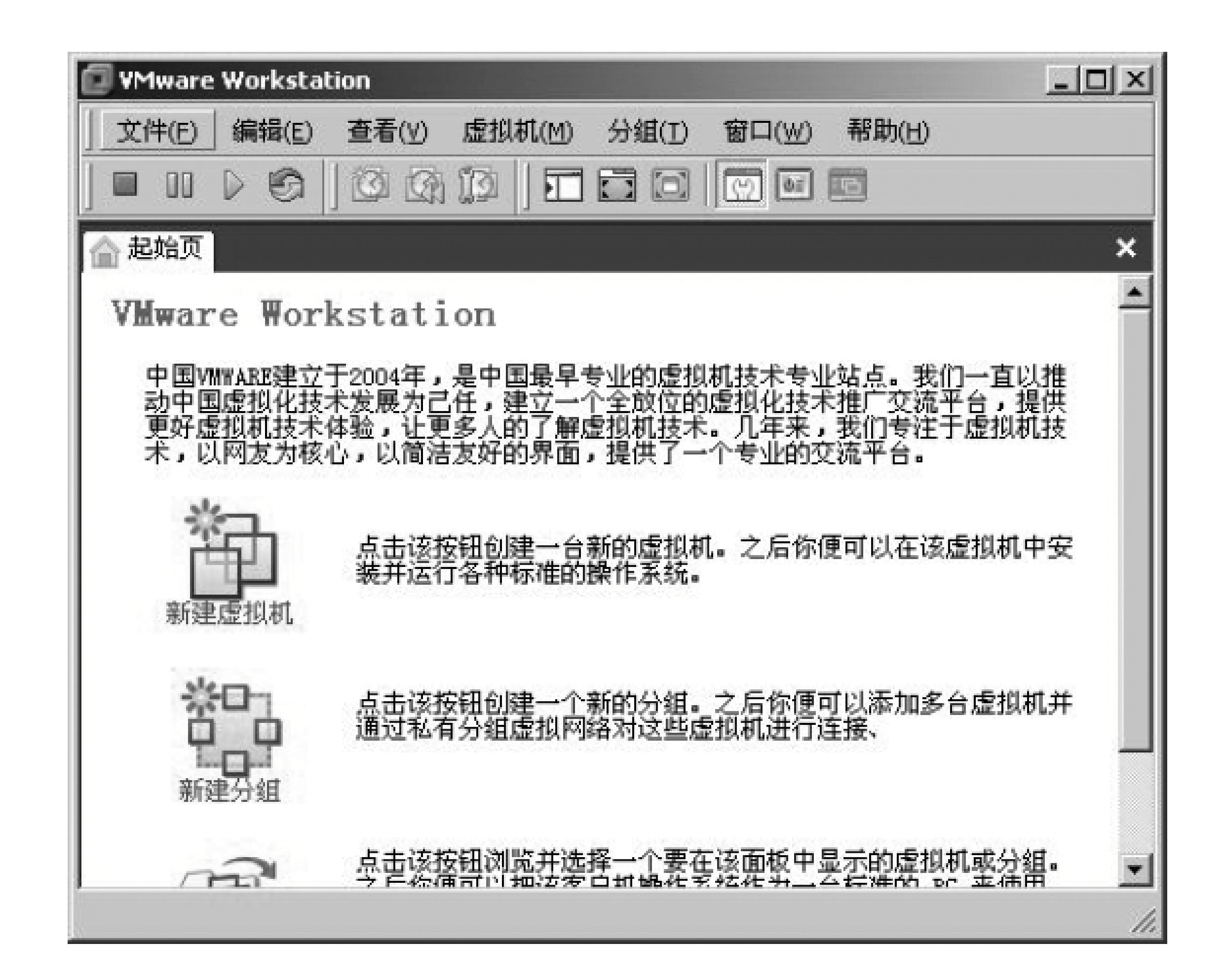


图 5-9　VMware Workstation 的【起始页】



图 5-10　选择操作系统类型



图 5-11　为虚拟机命名





（6）在【网络连接】选项区中选择【使用桥接网络】单选按钮，该选项表示此虚拟机的网卡是与物理网卡在同一个网络上，也就是可以连接到外部网络的网卡，如图 5-12 所示。

（7）选择虚拟机可用的硬盘空间，默认是 8GB，可以改变分配磁盘容量的大小，例如选择 6GB；选中【立即分配所有磁盘空间】复选框，单击【完成】按钮，如图 5-13 所示。

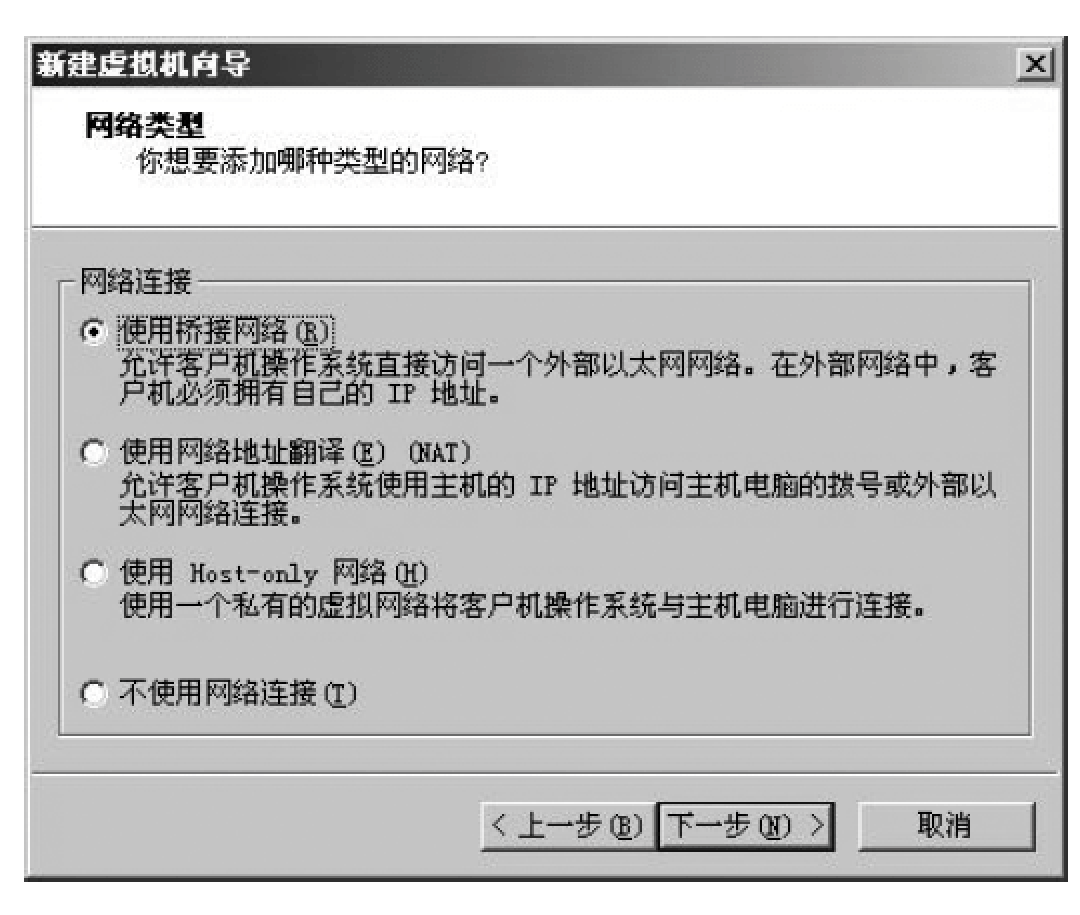


图 5-12　选择【网络连接】类型　　　　图 5-13　为虚拟机分配硬盘空间

（8）VMware 配置完成后，默认给虚拟机的内存是 384MB。如果读者的计算机系统内存足够大，建议设置为 512MB。可以通过双击图 5-14 右边【设备】列表框中的【内存】选项，打开对话框后改变内存的值。

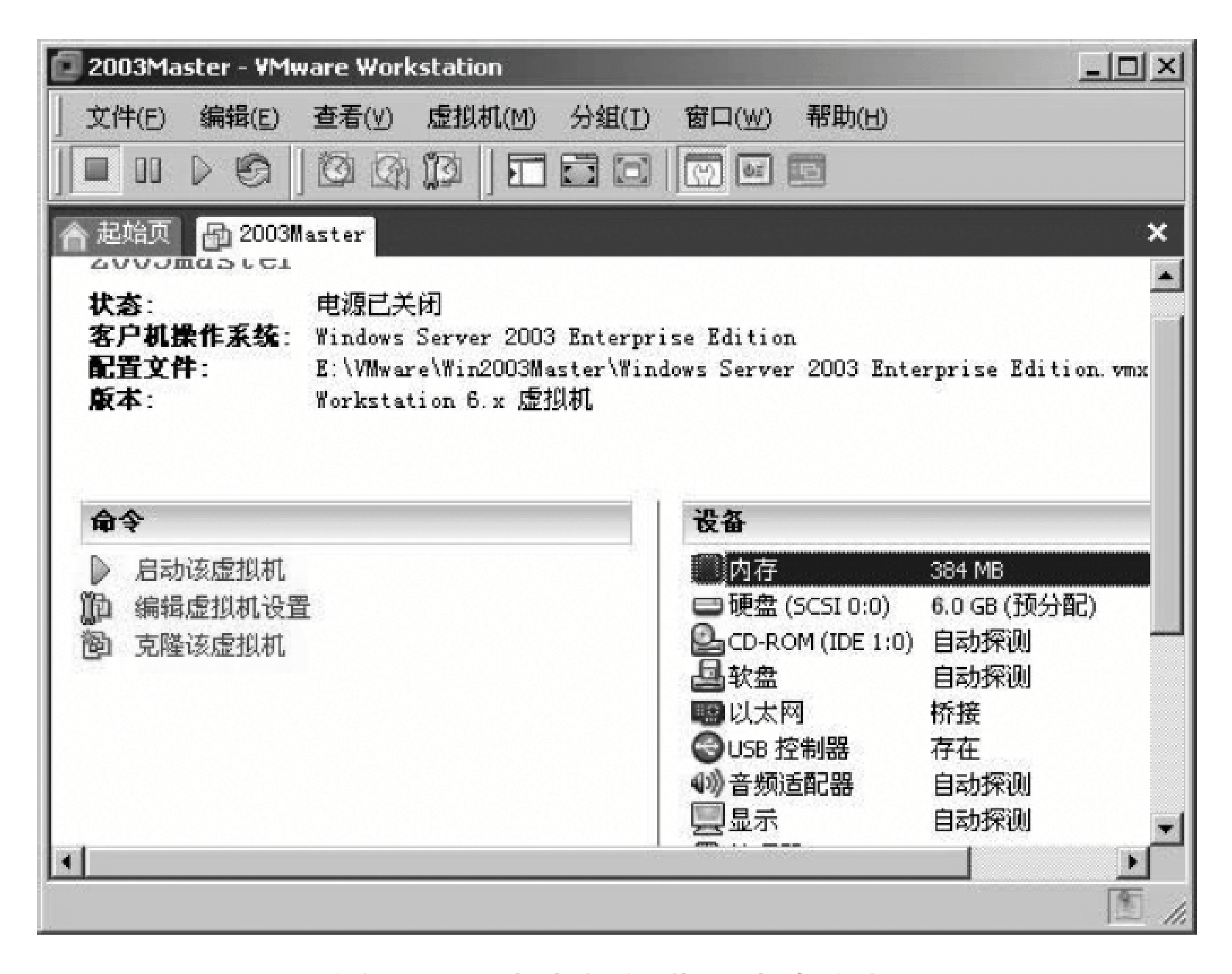


图 5-14　为虚拟机分配内存空间

3．启动虚拟机并安装 Windows Server 2003 操作系统

（1）将 Windows Server 2003 CD 放到光驱内（或者将用 Windows Server 2003 安装光盘制作的 ISO 文件加载到虚拟光驱内）。

（2）单击如图 5-15 所示的【启动该虚拟机】选项，之后开始安装 Windows Server 2003，



如图 5-16 所示。

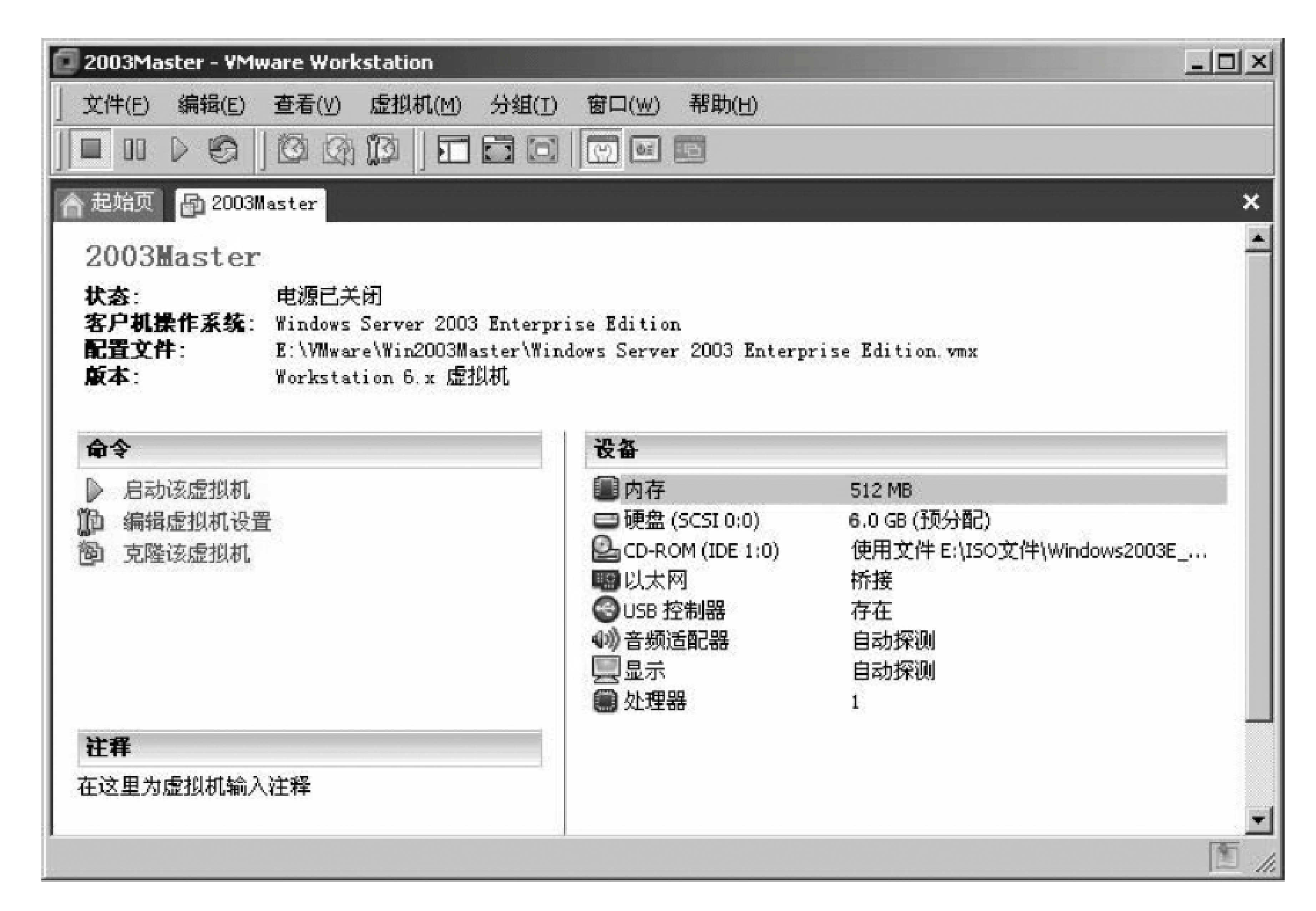


图 5-15　启动虚拟机

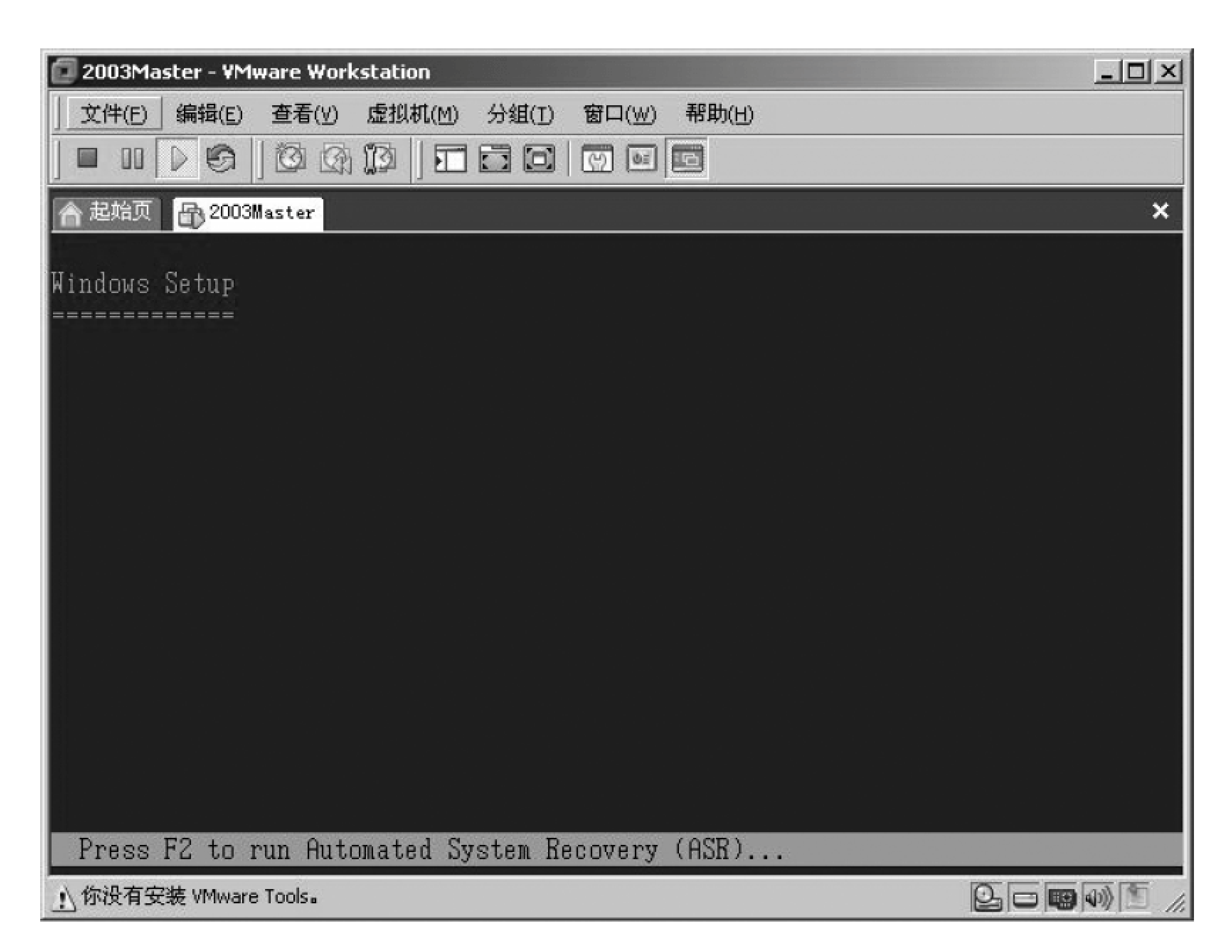


图 5-16　Windows Server 2003 安装界面

4. 安装 VMware Tools

如果没有安装 VMware Tools，就会有鼠标操作不顺的现象。在 Windows Server 2003 系统启动后，通过以下步骤来安装 VMware Tools：在 VMware Workstation 控制台画面中选择【虚拟机】/【安装 VMware Tools】命令，然后按照画面提示继续安装，如图 5-17 所示。





图 5-17　安装 VMware 工具

提示：可以在 VMware Workstation 控制台中，利用选择 VM/【按 Ctrl＋Alt＋Del】命令的方法来模拟按 Ctrl＋Alt＋Del 三个键的动作，或是直接按 Ctrl＋Alt＋Insert 组合键。

此虚拟机与操作系统的相关文件都保存在 E:\VMware 文件夹内，其中扩展名为.vmdk的文件约为 6GB，如图 5-18 所示。

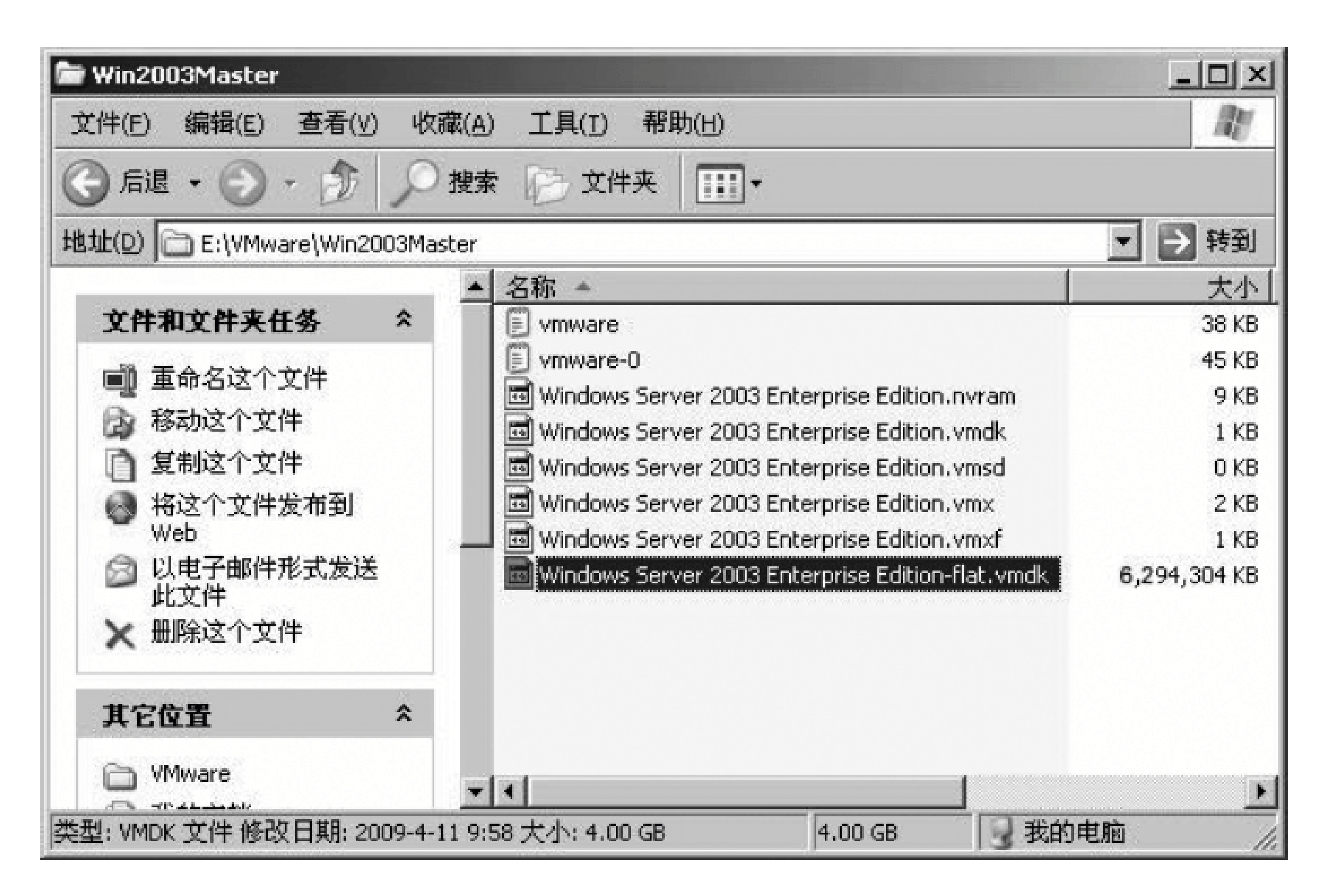


图 5-18　虚拟机相关文件

5．建立 ISA Server 2006 计算机的虚拟机

为了节省建立 ISA Server 2006 虚拟机与安装操作系统的时间，同时也为了节省硬盘空间，在此并不需要按照前面的步骤来建立虚拟机和安装操作系统，而是直接利用 VMware 的“克隆”功能克隆前面的虚拟机 2003Master。操作步骤如下：



（1）将虚拟机 2003Master 关机。

（2）单击 VMware Workstation 控制台中 2003Master 选项卡下的【克隆该虚拟机】选项，如图 5-19 所示。

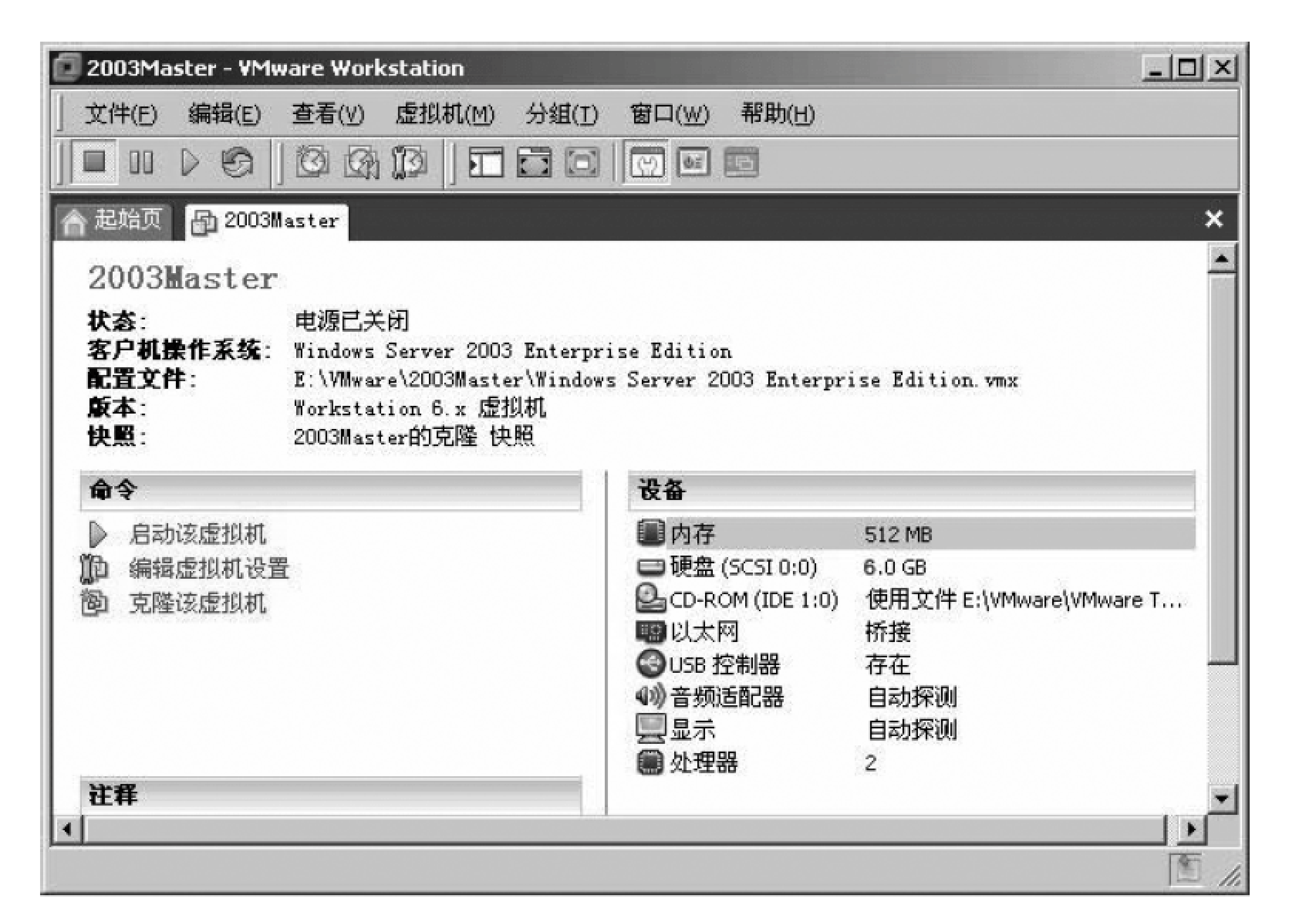


图 5-19　VMware Workstation 控制台

（3）在弹出的【克隆虚拟机向导】对话框中直接单击【下一步】按钮。

（4）在【克隆自】选项区中选择【虚拟机的当前状态】单选按钮后单击【下一步】按钮；在【克隆方式】选项区中选择【创建一个链接克隆】单选按钮并单击【下一步】按钮，如图 5-20 所示。

（5）为克隆的虚拟机取一个名称，例如 ISA Server 2006，如图 5-21 所示。

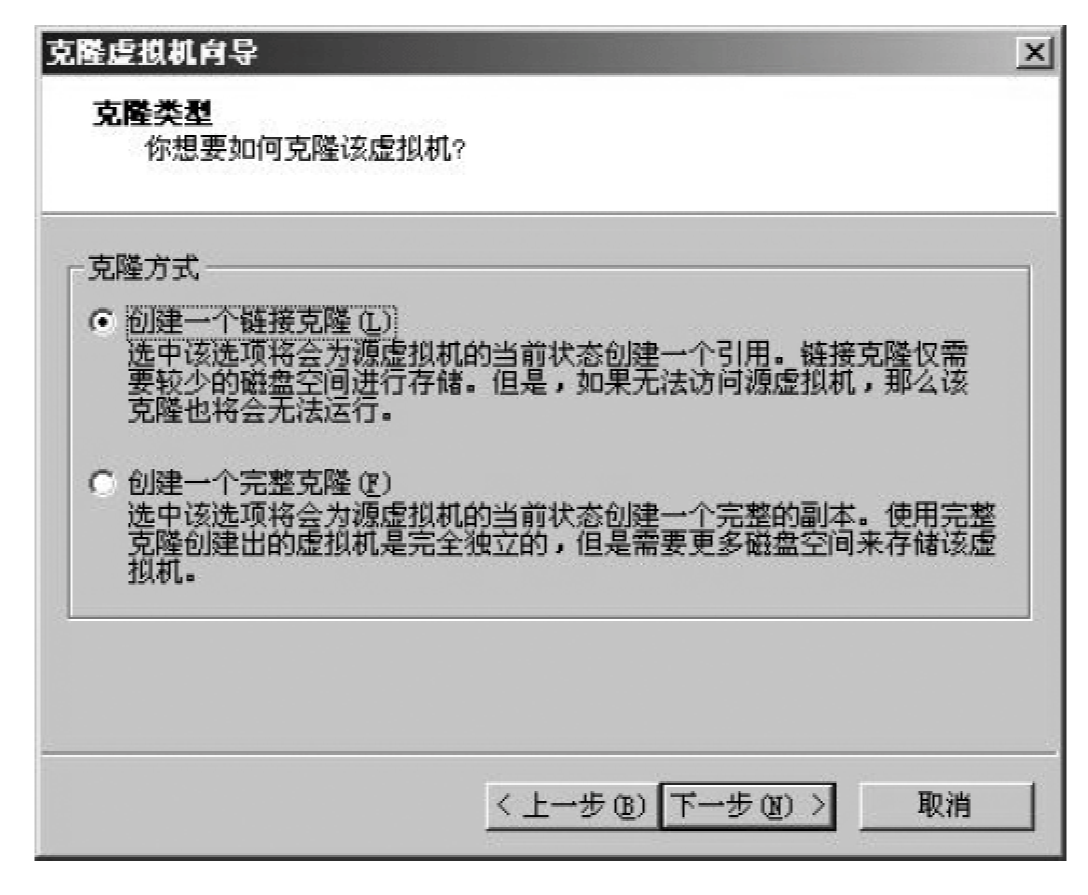


图 5-20　选择【克隆方式】



图 5-21　克隆的虚拟机名称

注意：将当做母盘的 2003Master 从 VMware Workstation 的控制台画面中删除不显示，以免不小心启动它并破坏其内的操作系统。不显示的方法是：选择 2003Master 选项卡中的【关闭】选项，这种方法不会删除此虚拟机，只是不显示而已，以后可以选择控制台菜单中的【文件】/【打开】命令的方法重新在控制台画面中显示此虚拟机。





6. 为 ISA Server 2006 计算机新建一张网卡

ISA Server 2006 虚拟机默认只有一张连接外部网络的虚拟网卡，还需要为此虚拟机新建一张连接内部网络的虚拟机网卡，即连接在 VMnet1(Host-only)虚拟网络上的网卡。方法如下：

(1) 在控制台画面选择 ISA Server 2006 选项卡中的【编辑虚拟机设置】选项，弹出【虚拟机设置】对话框，如图 5-22 所示。

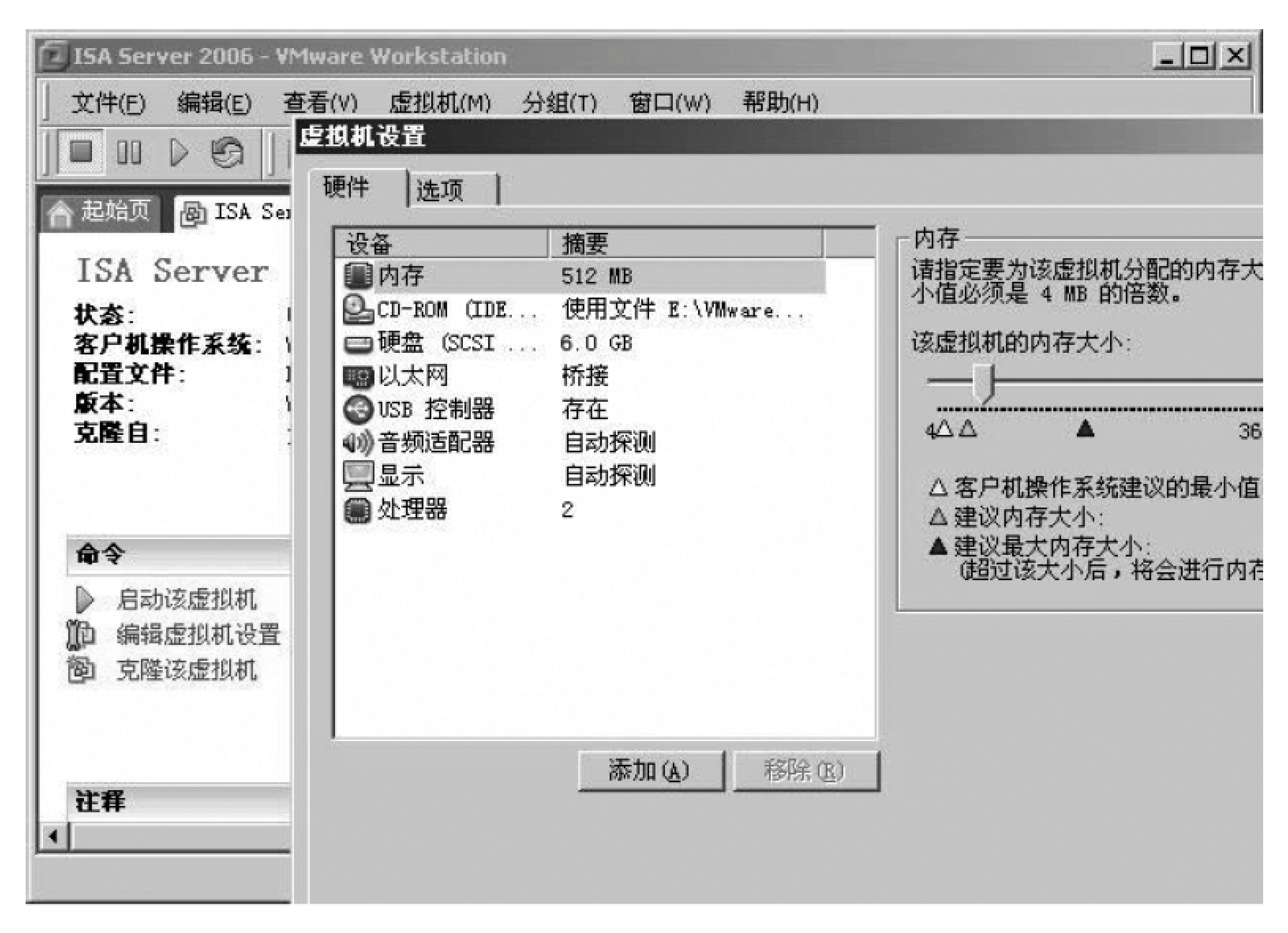


图 5-22　【虚拟机设置】对话框

(2) 单击【添加】按钮，在弹出的【添加硬件向导】对话框中从列表中选择"以太网适配器"选项，如图 5-23 所示。

(3) 单击【下一步】按钮，在【网络连接】选项区中选择 Host-only，也就是 VMnet1 虚拟网络，然后单击【完成】按钮，如图 5-24 所示。

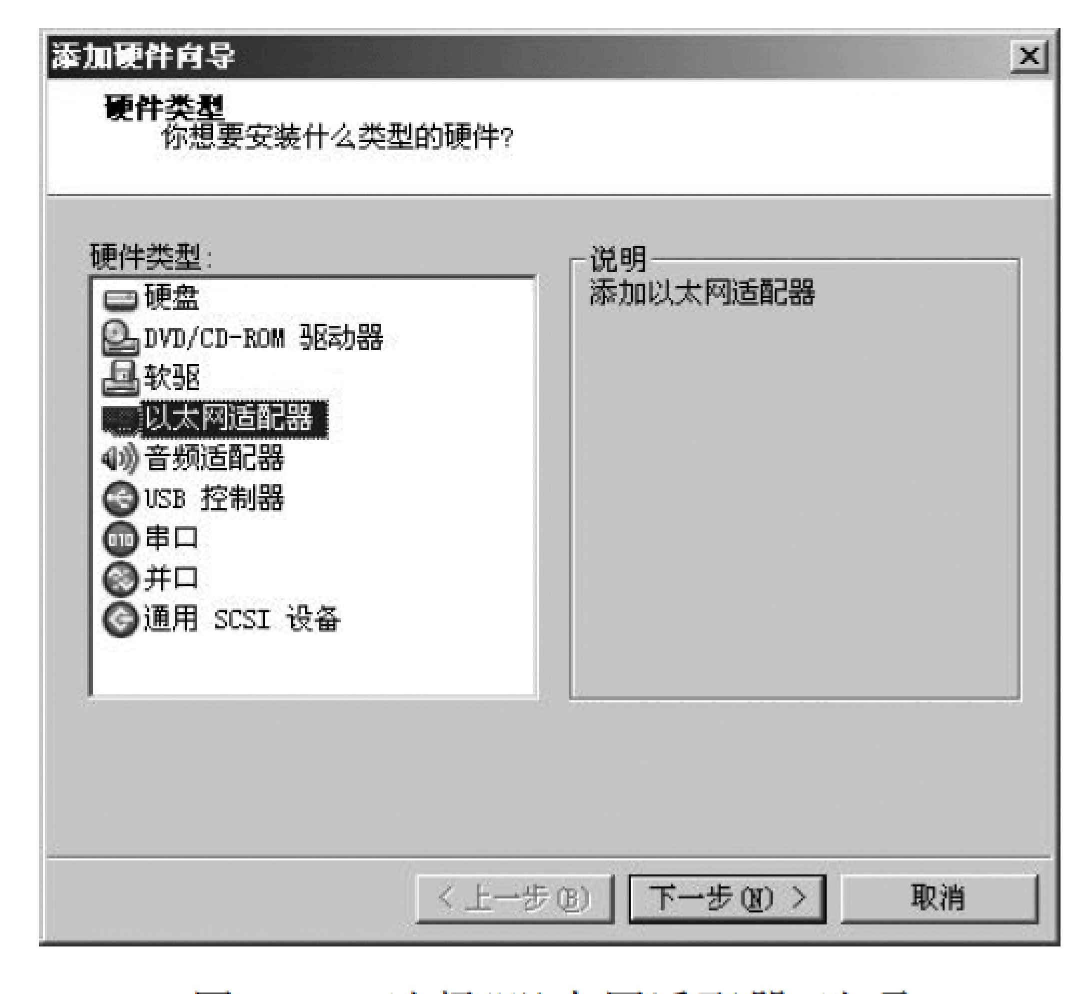


图 5-23　选择"以太网适配器"选项



图 5-24　选择网络连接类型



（4）完成后的画面如图 5-25 所示。

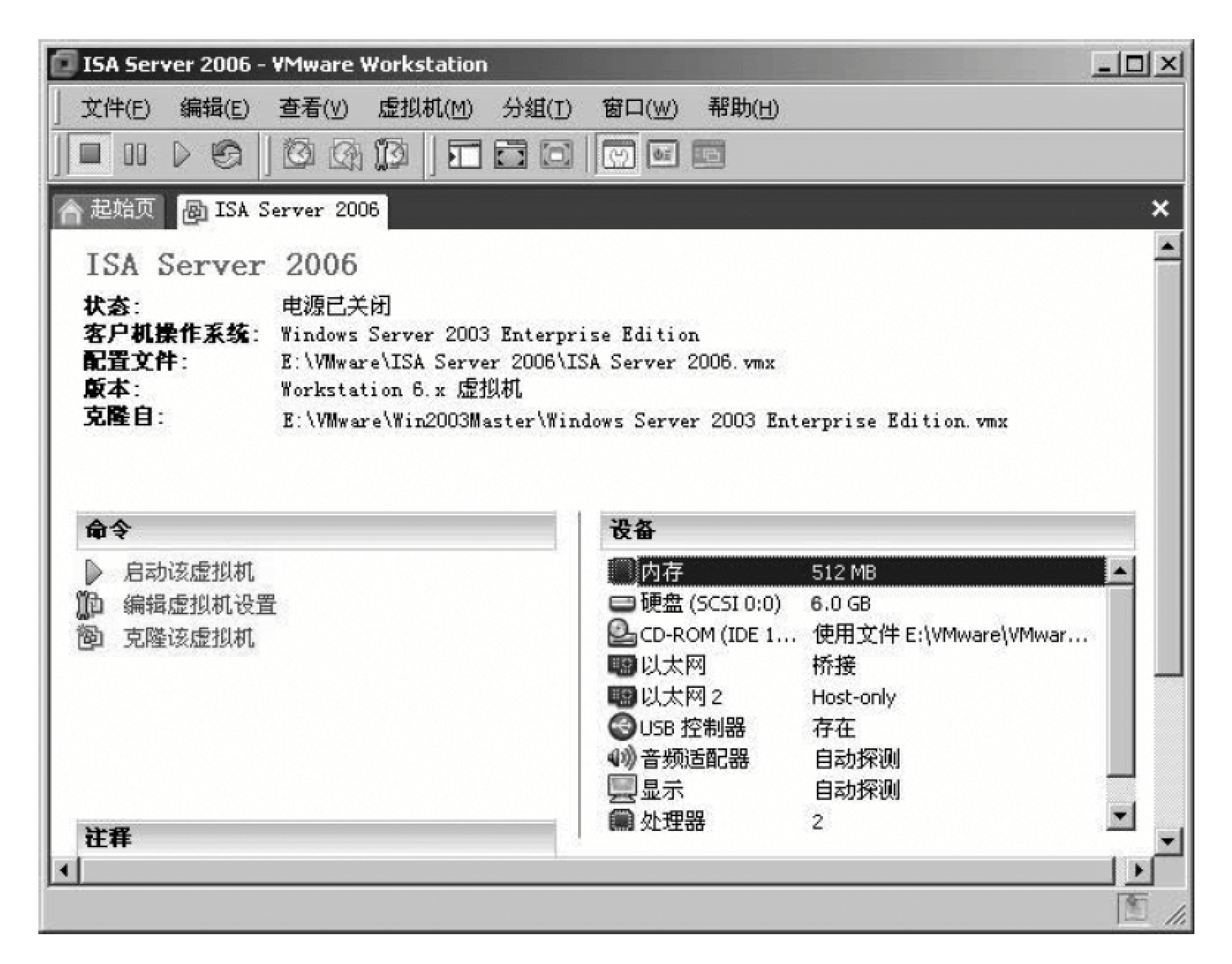


图 5-25　添加了“以太网 2”网卡

5.3　ISA 网络配置和网络规则

ISA Server 程序安装好后，就可正式对服务器端各方面进行配置了。首先要配置的是网络。ISA Server 2006 支持多网络（多个网络可以组成“网络集”），所以对 ISA 网络的配置实际上就是对网络集中各个具体网络的配置。

5.3.1　网络和网络集配置

从 ISA Server 的角度看，网络是一个规则的最小元素，它可以包含一个或多个 IP 地址范围。网络包含一台或多台计算机，并对应于物理网络。可以将定义的规则应用于一个或多个网络，或者应用于除指定网络中的地址以外的所有地址。

1. ISA 网络类型

ISA Server 2006 内建了以下 5 种网络，如图 5-26 所示。下面分别说明。

（1）本地主机。本地主机就是指 ISA Server 这台计算机，不能修改或删除本地主机网络。从严格意义上说，不能称之为网络，因为它只有一台计算机。出入 ISA Server 的所有通信都被认为是通过本地主机网络传递的。

与任何网络一样，必须在本地主机网络与其他网络之间指定一种关系。默认的“本地主机访问”网络规则指定了本地主机网络与其他网络之间的路由关系。在定义了防火墙策略和网络规则后，只允许从本地主机网络访问通常驻留在其他网络中的基本服务。由于其中





图 5-26　ISA 内建的 5 种网络

的许多服务对于 ISA 服务器的基本功能至关重要，因此在安装 ISA 服务器时创建的一组默认系统策略规则允许访问这些服务。

（2）内部网络。一般来说，内部网络就是指内部的局域网。安装后，此网络将包含安装过程中指定的所有计算机（IP 地址）。不能删除内部网络。

由 ISA 服务器使用的内部网络代表主要的默认受保护网络。可以指定多个其他内部网络。在安装时至少要配置一个默认内部网络。默认情况下，系统策略规则防止从其他所有网络（而不是本地主机网络）访问内部网络上的资源。可以创建访问规则和发布规则，前者允许从默认内部网络到其他网络进行通信，后者允许访问位于内部网络上的服务器。

通常认为内部网络包含受信任的网络，为此，默认系统策略允许 ISA 服务器访问内部网络上的服务。

边界网络就是 DMZ（Demilitarized Zone，中文名称为“隔离区”，也称“非军事化区”）。一般将边界网络归为内部网络。

（3）外部网络。除了已经定义的网络（例如内部网络（包括边界网络）VPN 客户端等）之外，其他所有的网络都属于外部网络。

此网络包含不与其他任何网络关联的所有计算机（IP 地址），也不能修改或删除外部网络。外部网络是 ISA Server 安装后配置的 5 个网络之一。外部网络包含未明确包含在其他任何网络中的所有 IP 地址。安装时，外部网络包含所有未包含在内部网络中的地址、本地主机网络的 IP 地址，以及 ISA Server 计算机上除了内部网络外的其他所有网络适配器的 IP 地址。

通常将外部网络视为不受信任的网络，因此，通常将其他网络（称之为“源网络”）与默认外部网络的网络关系配置为网络地址转换（NAT），从而允许源网络上的客户端访问目标默



认外部网络，但是却防止默认外部网络访问源网络。

(4) VPN 客户端。VPN 客户端连接到 ISA Server(VPN 服务器)后，它们会被归纳到这个被称为 VPN 客户端的网络，此网络包含当前连接的客户端的地址。当配置虚拟专用网络(VPN)属性时，将配置可能地址范围。不能删除 VPN 客户端网络。

要通过使用 ISA Server 来允许远程虚拟专用网络(VPN)客户端，必须启用 VPN 客户端访问。当启用 VPN 客户端访问时，ISA Server 启用适当的网络和防火墙策略规则以允许初始访问。当允许远程 VPN 客户端连接时，ISA Server 使这些客户端成为 VPN 客户端网络的成员。默认系统策略规则允许这些客户端访问 ISA 服务器(本地主机网络)。

(5) 被隔离的 VPN 客户端。如果在 ISA Server 上启用了隔离控制的功能，则可以要求 VPN 客户端必须符合规定，例如 VPN 客户端必须安装防毒软件、必须安装最新的补丁等。当 VPN 客户端连接到 ISA Server 时，它们会先被暂时归纳到隔离的 VPN 客户端网络，等到它们通过检查后，才会被归纳到 VPN 客户端网络，如果客户端无法通过检查，就会继续被隔离在隔离的 VPN 客户端网络。

要允许访问某项资源，可以创建访问规则，以被隔离的 VPN 客户端网络为源，并以需要访问的服务器为目标。为此，需要为每台服务器创建计算机规则元素，以便它可以在访问规则中使用。或者可以创建一个计算机集，其中包含已隔离客户端需要访问的所有计算机；同时创建访问规则，以被隔离的 VPN 客户端网络为源，并以计算机集为目标。另外一种方法是对网络进行设计，使需要访问的所有服务器都属于一个子网，然后定义一个在访问规则中使用的子网规则元素。

2. 创建网络

除了上述预安装的网络外，用户还可以自己创建所需的新网络。可以选择要创建的网络类型有内部(含边界)、外部和 VPN 站点到站点这几种。创建的新网络将自动包含在“所有受保护网络”网络集中。选择上述某一种网络类型后，可以指定要包含在该网络中的 IP 地址。要注意的是，每个 IP 地址只能包含在一个网络中。

3. 网络集

创建网络后，可以将一个或多个网络组织成网络集。网络集可以包含一个或多个网络，或者可以明确地排除一个或多个网络。规则可以应用于网络或网络集。

安装 ISA Server 时，默认创建两个网络集，如图 5-27 所示。不能修改或删除以下这两个网络集。

(1) 所有网络。此网络集包含为 ISA Server 定义的所有网络，创建的新网络将自动包含在此网络集中。

(2) 所有受保护的网络。此网络集包含除内置外部网络以外的所有网络，创建的新网络将自动包含在此网络集中。

5.3.2 应用网络模板

ISA Server 包含与常见网络拓扑对应的五种网络模板(参考 5.1.3 小节)，用户在安装 ISA Server 系统时，ISA Server 会自动根据用户当前的网络环境和配置选择一种默认的模板。





图 5-27　默认网络集

如果用户改变了网络环境和配置，或者觉得 ISA Server 自动选择的网络模板不符合要求，用户也可以根据自己的网络环境和应用需求选择应用其中一种网络模板，为网络之间的通信配置防火墙策略，如图 5-28 所示。



图 5-28　应用网络模板

5.3.3　网络规则

网络规则确定了在两个网络实体之间是否存在着关系，以及属于哪种类型的网络关系。



在 ISA 的网络集中包括了几种网络类型，它们之间相互关联，从而形成一个网络集。如果未配置网络之间的关系，那么 ISA Server 将丢弃两个网络之间的所有通信。使用 ISA Server 来配置网络规则，可定义并描述网络拓扑。

1. 网络关系

网络规则中涉及两种网络关系，那就是路由和网络地址转换。

(1) 路由。当指定这种类型的连接时，来自源网络的客户端请求将被直接转发到目标网络，源客户端地址包含在请求中。

路由网络关系是双向的，如果在从网络 A 到网络 B 这一方向上定义了路由关系，那么在从网络 B 到网络 A 这一方向上也存在着路由关系。

(2) 网络地址转换(NAT)。当指定这种类型的连接时，ISA Server 将用它自己的 IP 地址替换源网络中的客户端的 IP 地址。

NAT 网络关系是单向的、唯一的，如果在从网络 A 到网络 B 这一方向上定义了 NAT 关系，那么便不能在从网络 B 到网络 A 这一方向上定义网络关系。

2. 默认规则

ISA Server 在安装时会创建一些默认的网络规则，如图 5-29 所示。



图 5-29　默认网络规则

(1) 本地主机访问。此规则定义了在本地主机网络与其他所有网络之间存在的路由关系。这样，便在 ISA Server 计算机与连接到该 ISA Server 计算机的所有网络之间定义了连接性。

(2) VPN 客户端到内部网络。此规则定义了在内部网络与被隔离的 VPN 客户端以及 VPN 客户端网络之间存在的路由关系。



（3）Internet 访问。此规则定义了在内部网络与外部网络之间存在的 NAT 关系。

3. 网络规则的处理顺序

网络规则是有顺序的。为了确定两个地址 A 和 B 之间的地址关系，ISA Server 按照优先级顺序处理网络规则，查找与地址匹配的规则。地址关系由匹配的第一条规则指定，这意味着可以在两个网络之间定义具有路由关系的网络规则，然后再通过创建一条优先级更高的网络规则来替代特定地址的这一关系。

4. 创建网络规则

创建网络规则时，不能在网络与其自身之间指定网络规则。同一网络中的计算机之间的通信被指定为路由关系，不支持 NAT 关系。

5.4　安装 ISA Server 2006

5.4.1　安装前的准备

ISA Server 2006 企业版只能在 Windows Server 2003 SP1 和 R2 版本中安装，不能在 64 位版本的 Windows Server 2003 操作系统上安装 ISA Server 2006。但如果 ISA Server 2006 是作为域成员安装的，则 ISA Server 企业版仅可以安装在 Windows Server 2003 或 Windows Server 2000 域中。

1. ISA Server 2006 企业版安装前的考虑

开始安装之前，应考虑 ISA Server 2006 Enterprise Edition 基础结构的拓扑，同时考虑以下事项。

- 是否要在工作组或受信任的域环境中部署 ISA Server。
- 要将配置存储服务器安装在何处。
- 是否要将所有配置存储服务器安装在同一个站点中。
- 是否要远程管理企业。
- 安装多少台远程管理计算机。
- 至少一个 NTFS 格式的磁盘分区，用于 ISA Server 缓存磁盘配额配置。

2. ISA Server 2006 企业版服务器的部署思路

安装 ISA Server 之前，请按照以下步骤部署计算机。

（1）安装配置存储服务器。只有配置存储服务器可用，才能安装 ISA Server 2006 组件。在安装配置存储服务器时，可以将该服务器加入到现有企业。另外，还可以创建新的企业。为了获得最有效的部署，建议在你的组织中创建单一企业。使用单一企业，可以从一个 ISA 服务器管理 MMC 管理单元管理组织中的所有阵列。

（2）在配置存储服务器中创建阵列、企业网络规则和企业策略。当按下一步骤所述开始安装阵列成员时，可以将其加入到已存在的阵列中。



(3) 在一台或多台计算机上安装 ISA Server 服务。如果运行 ISA Server 服务的计算机是新阵列的第一个成员,则安装时需要在内部网络中指定地址。

3. 准备好 VMware Workstation 虚拟机

按照 5.2 节的要求搭建好 ISA Server 2006 的测试环境。

5.4.2 安装 ISA Server 2006

1. 更改 ISA Server 虚拟机的 SID

启动用来安装 ISA Server 2006 的虚拟机(之前克隆的 ISA Server 2006 虚拟机)。由于这台虚拟机是从 2003Master 复制出来的,所有虚拟机的 SID(Security Identifier,安全标识符)都是相同的,因此需更改这台 ISA Server 2006 虚拟机的 SID。登录 http://www.microsoft.com/zh/cn/,搜索与下载工具程序 NewSID,解压缩后执行 NewSID.EXE,然后在图 5-30 中单击 Next 按钮,在图 5-31 中重新为此计算机设置新的计算机名称,完成更改后系统将自动重新启动。

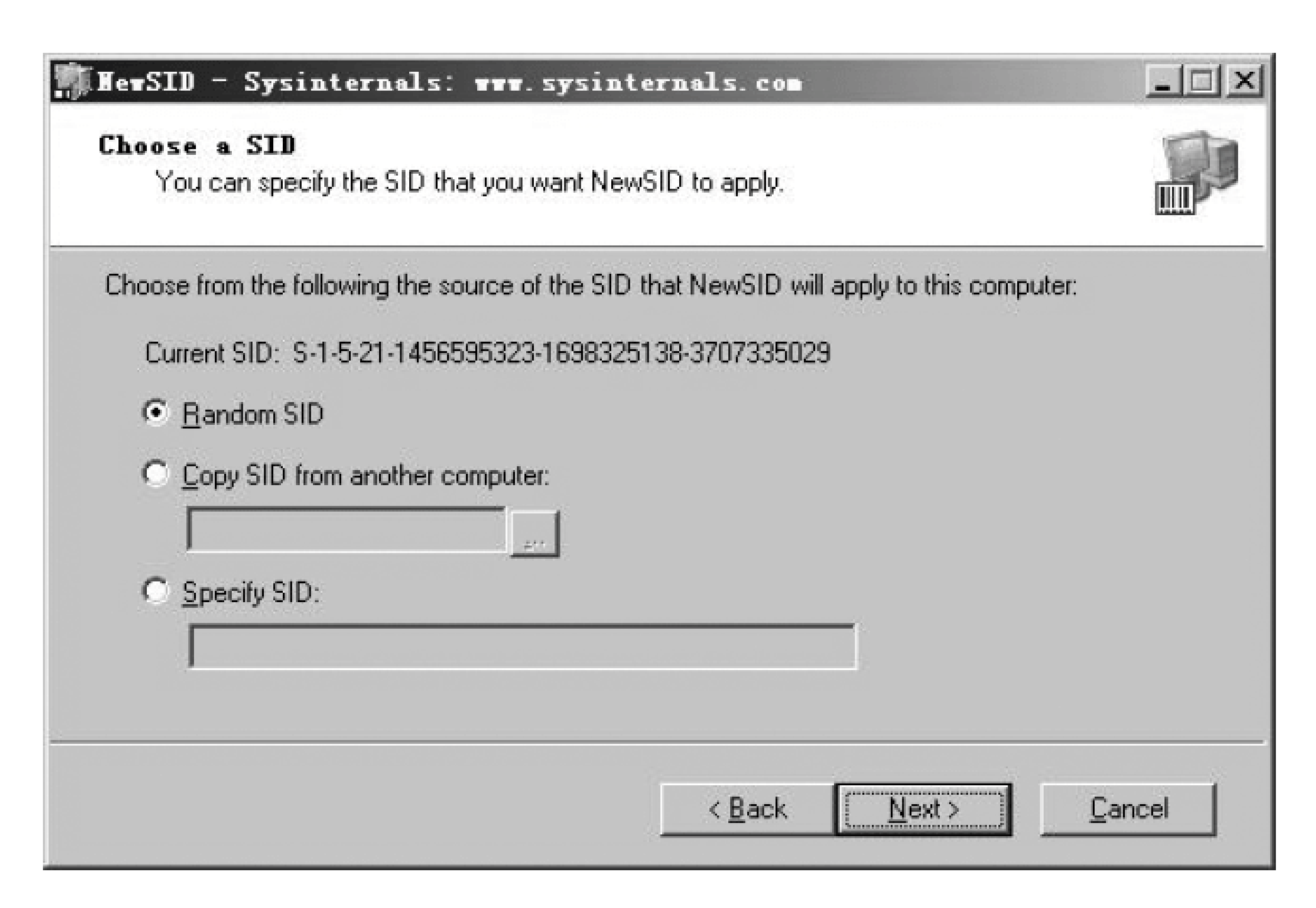


图 5-30 更改虚拟机的 SID

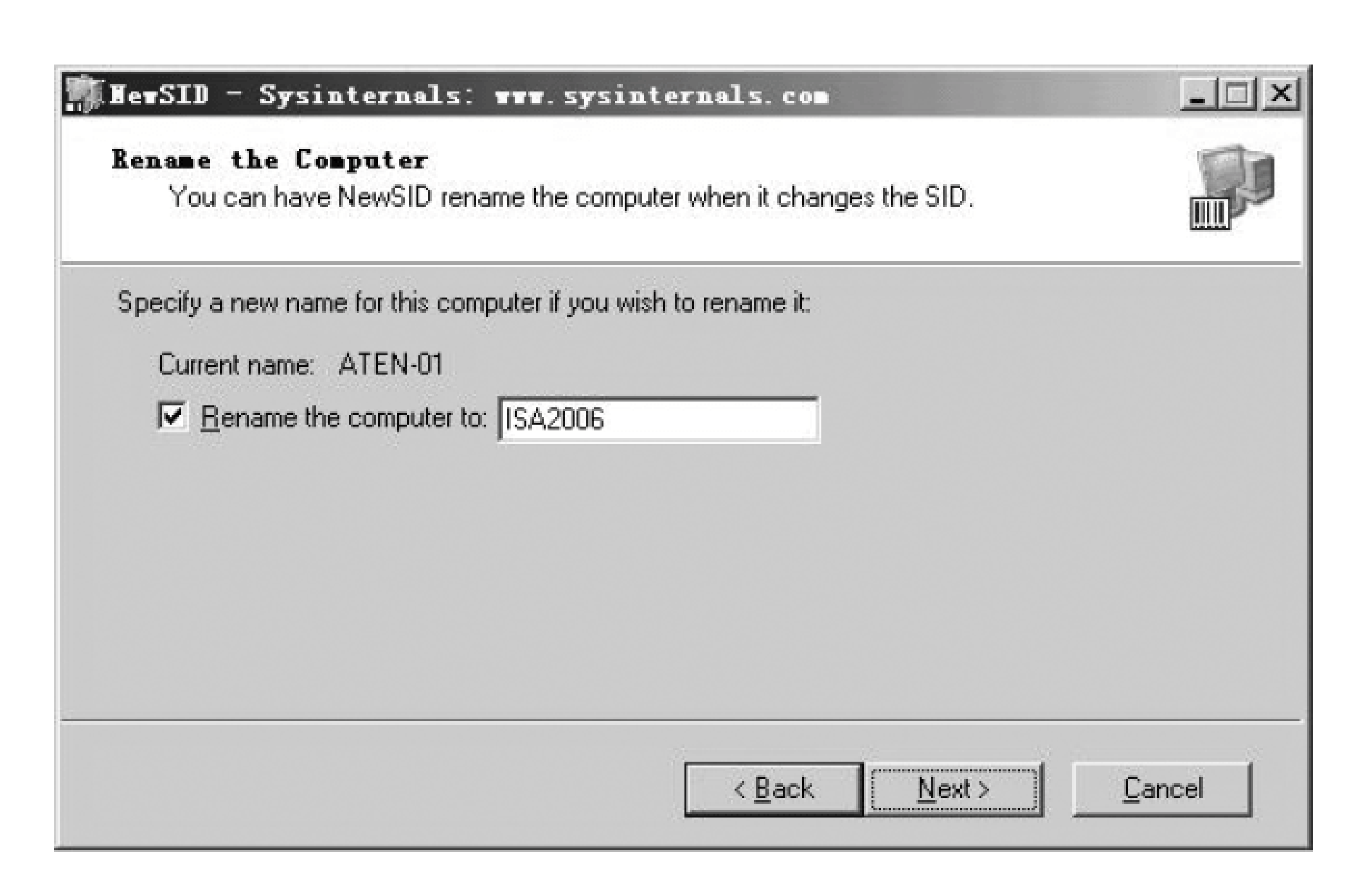


图 5-31 设置新的计算机名称



2. 更改网络名称与设置 IP 地址

本实验将以图 5-32 为例来说明如何将 ISA Server 2006 企业版安装到图中的 ISA Server 防火墙计算机上。

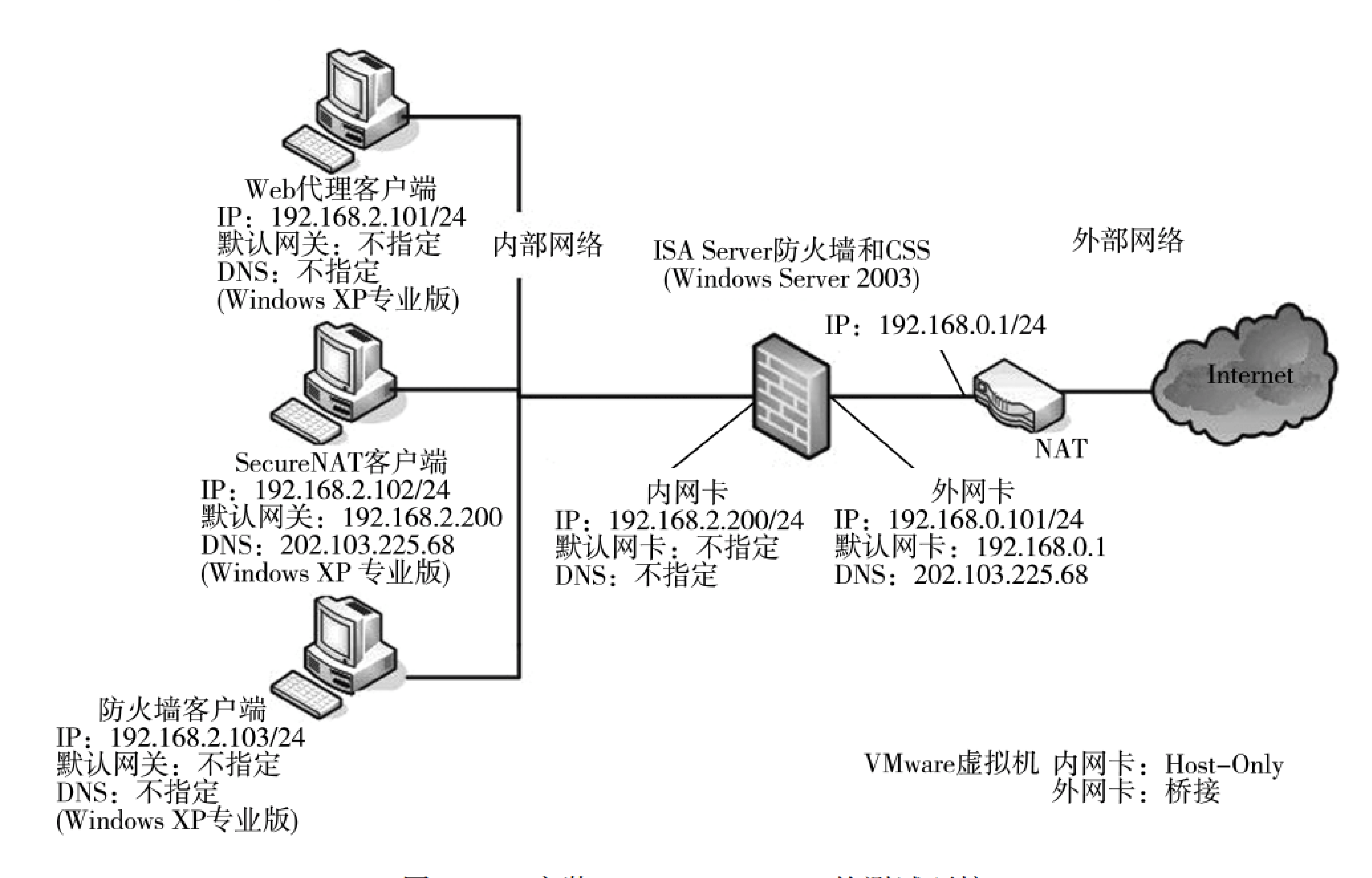


图 5-32　安装 ISA Server 2006 的测试环境

为了易于辨别，本实验将更改 ISA Server 2006 这台虚拟机的网卡名称。将这台虚拟机连接外部网络的网卡（桥接网卡）改名为“外网卡”，连接内部网络的网卡（Host-only 网卡）改名为“内网卡”。如图 5-33 所示是 ISA Server 虚拟机网卡更名前的画面，如图 5-34 所示是网卡更名后的画面。



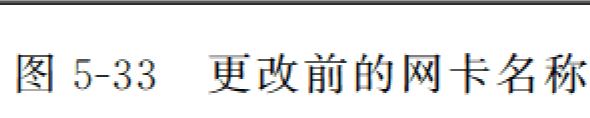

图 5-33　更改前的网卡名称



图 5-34　更改后的网卡名称

另外，参照如图 5-35 所示设置外网卡的 IP 参数，让这台 ISA Server 2006 虚拟机可以连接到 Internet，而内网卡的 IP 参数可参照图 5-36 所示设置。



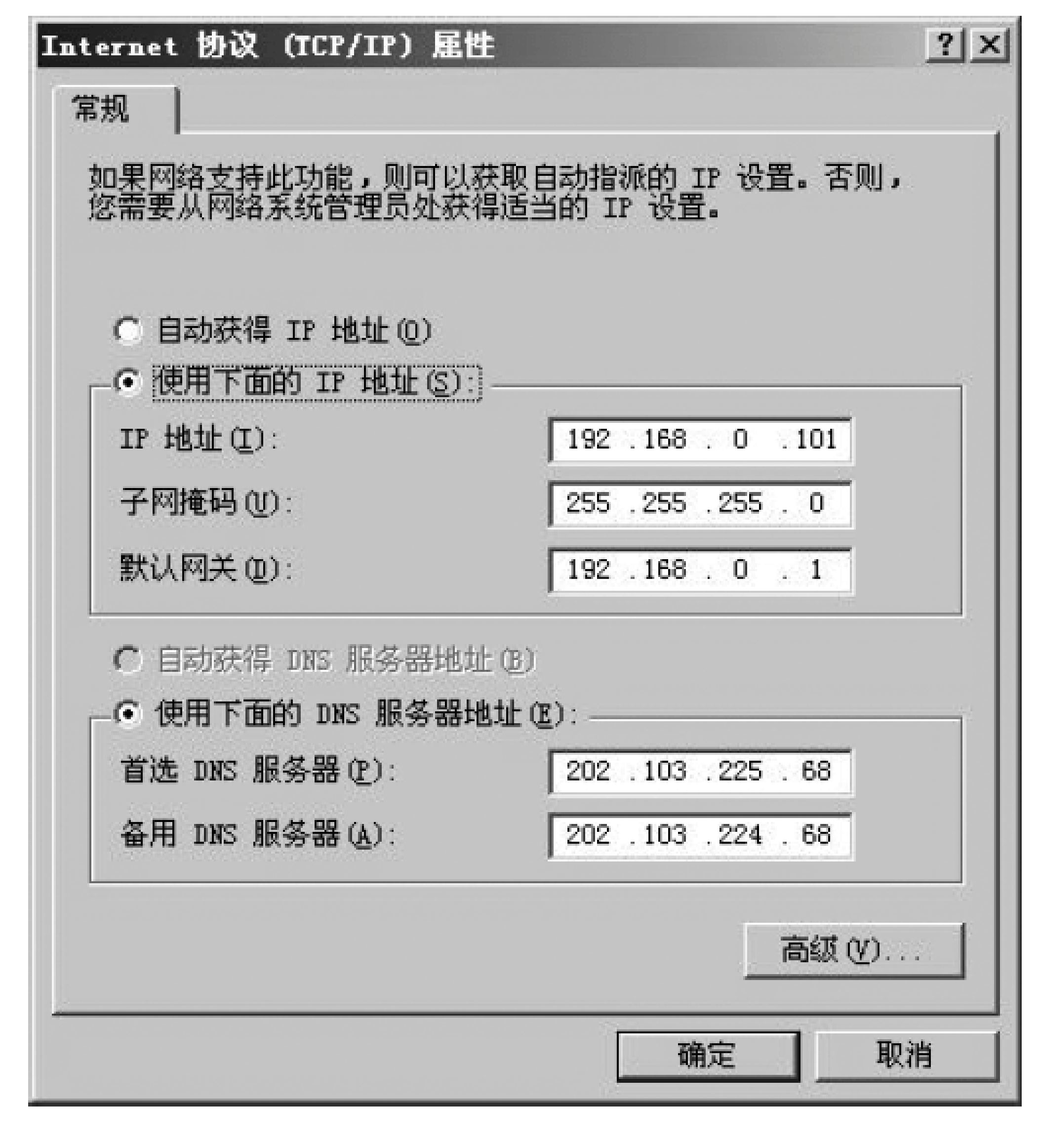


图 5-35 外网卡的 IP 地址设置

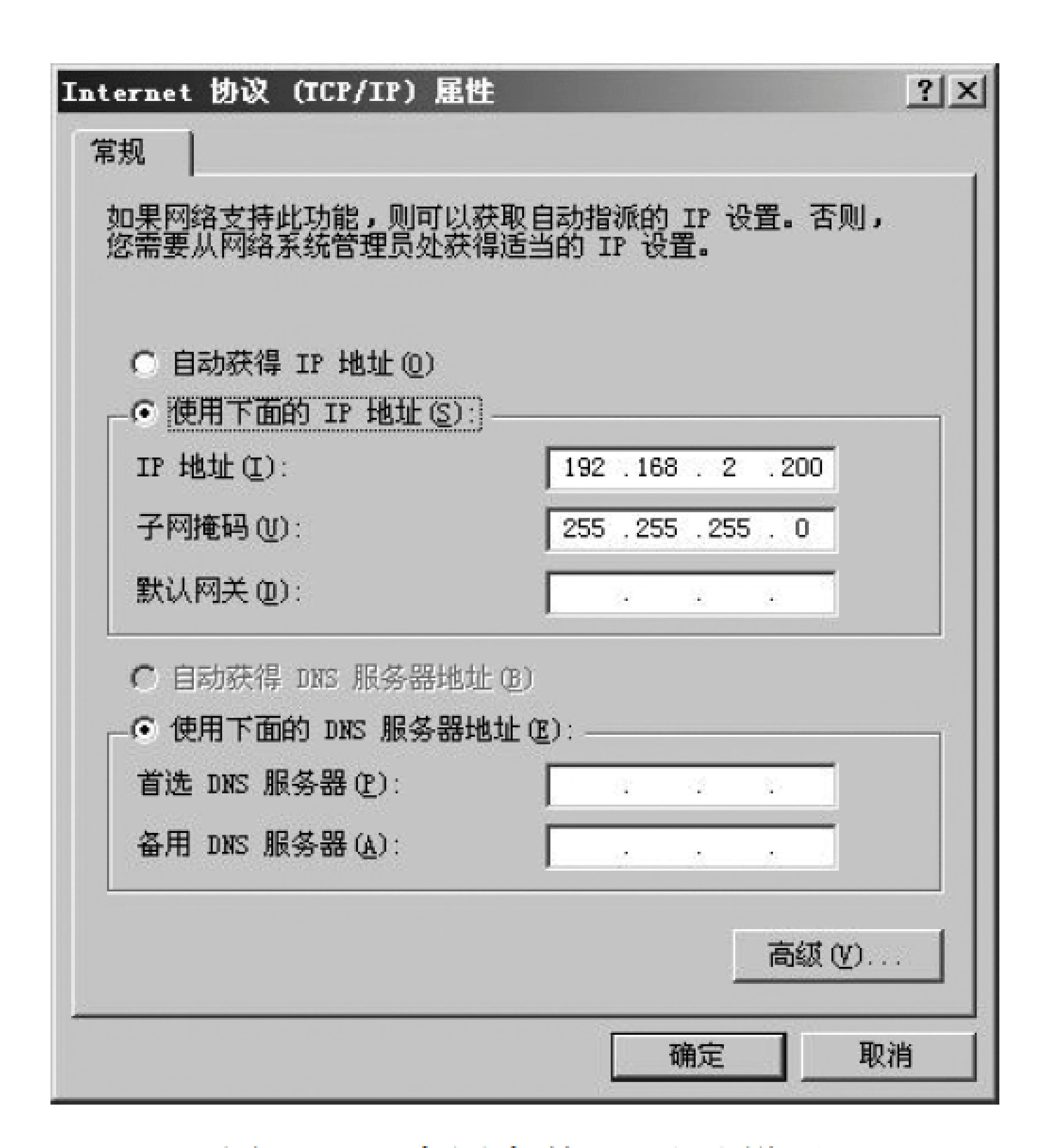


图 5-36 内网卡的 IP 地址设置

3．安装 ISA Server 2006

(1) 将 ISA Server 2006 企业版 CD 放到光驱内，以便自动启动安装程序，或者执行安装文件中的 ISAAutorun. exe 程序。

(2) 如图 5-37 所示，单击【安装 ISA Server 2006】选项。

(3) 在弹出的对话框中单击【下一步】按钮，在【许可协议】对话框中选择【我接受许可协议】选项，单击【下一步】按钮。

(4) 在【客户信息】对话框中输入用户名称、产品序号后，单击【下一步】按钮。

(5) 在图 5-38 中选择【同时安装 ISA Server 服务和配置存储服务器】后单击【下一步】按钮。

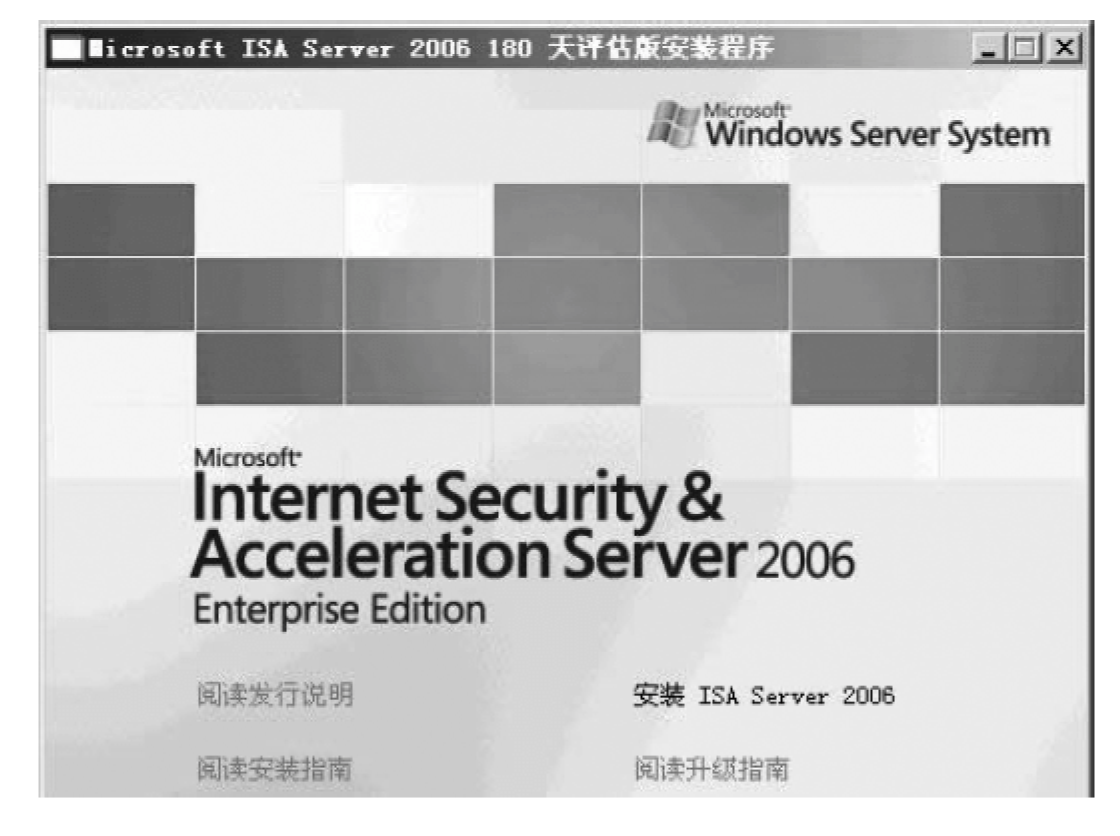


图 5-37 安装 ISA Server 2006

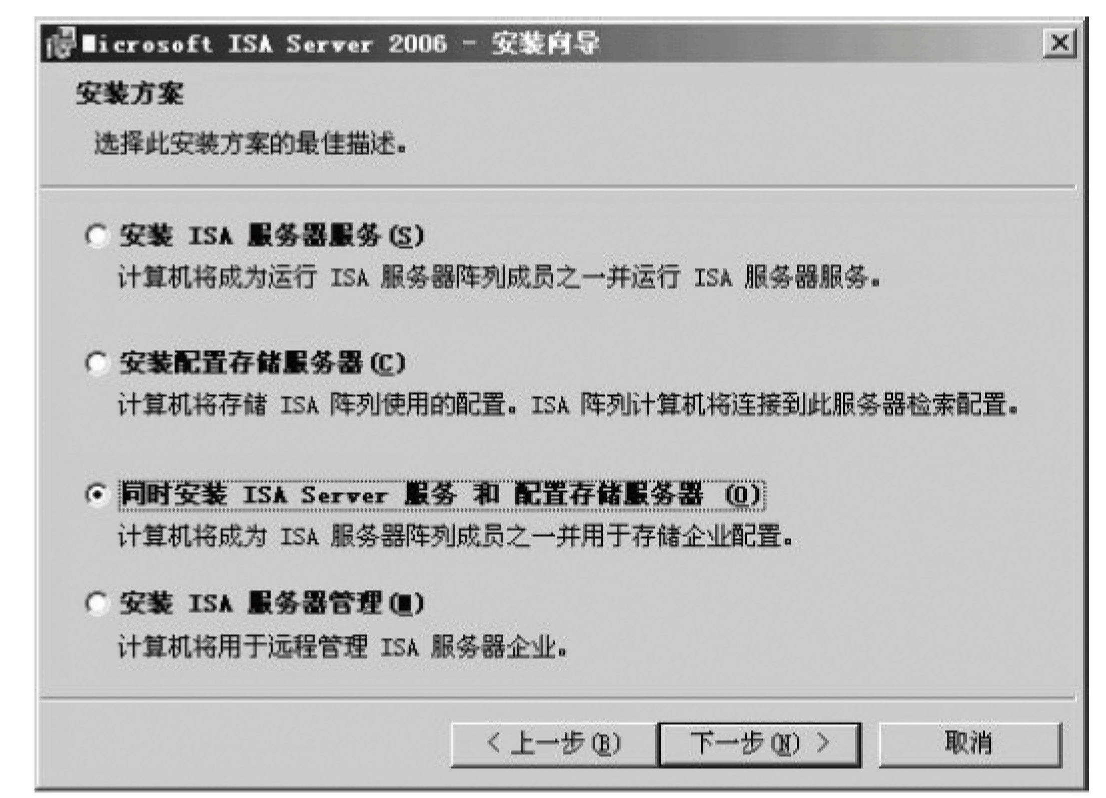


图 5-38 选择【安装方案】

(6) 在图 5-39 中直接单击【下一步】按钮。

(7) 在图 5-40 中采用默认的【创建新 ISA 服务器企业】后单击【下一步】按钮。





图 5-39 选择安装组件

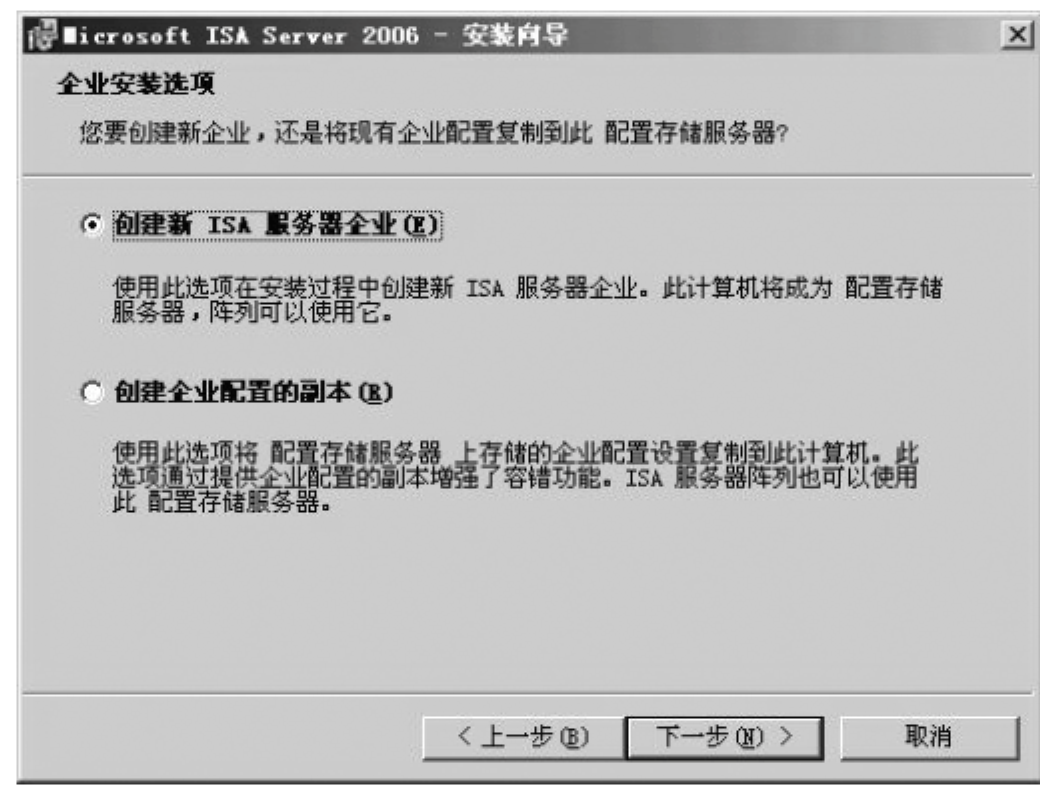


图 5-40 选择企业安装选项

（8）在图 5-41 中直接单击【下一步】按钮。建议在此对话框中最好只建立一个企业，否则将很难集中管理所有阵列中的计算机。

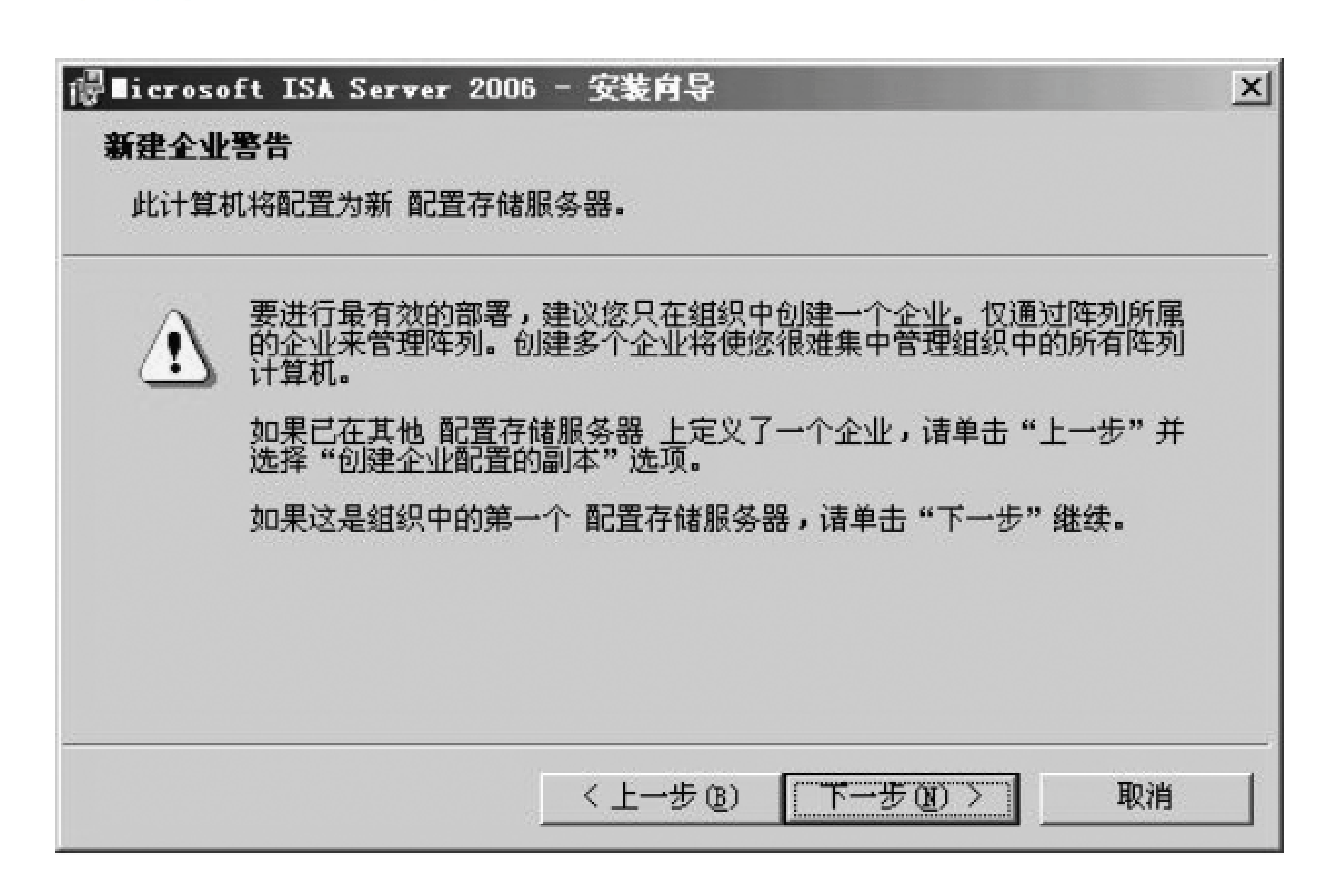


图 5-41 【新建企业警告】对话框

（9）在图 5-42 中单击【添加】按钮，指定内部网络的 IP 地址范围。

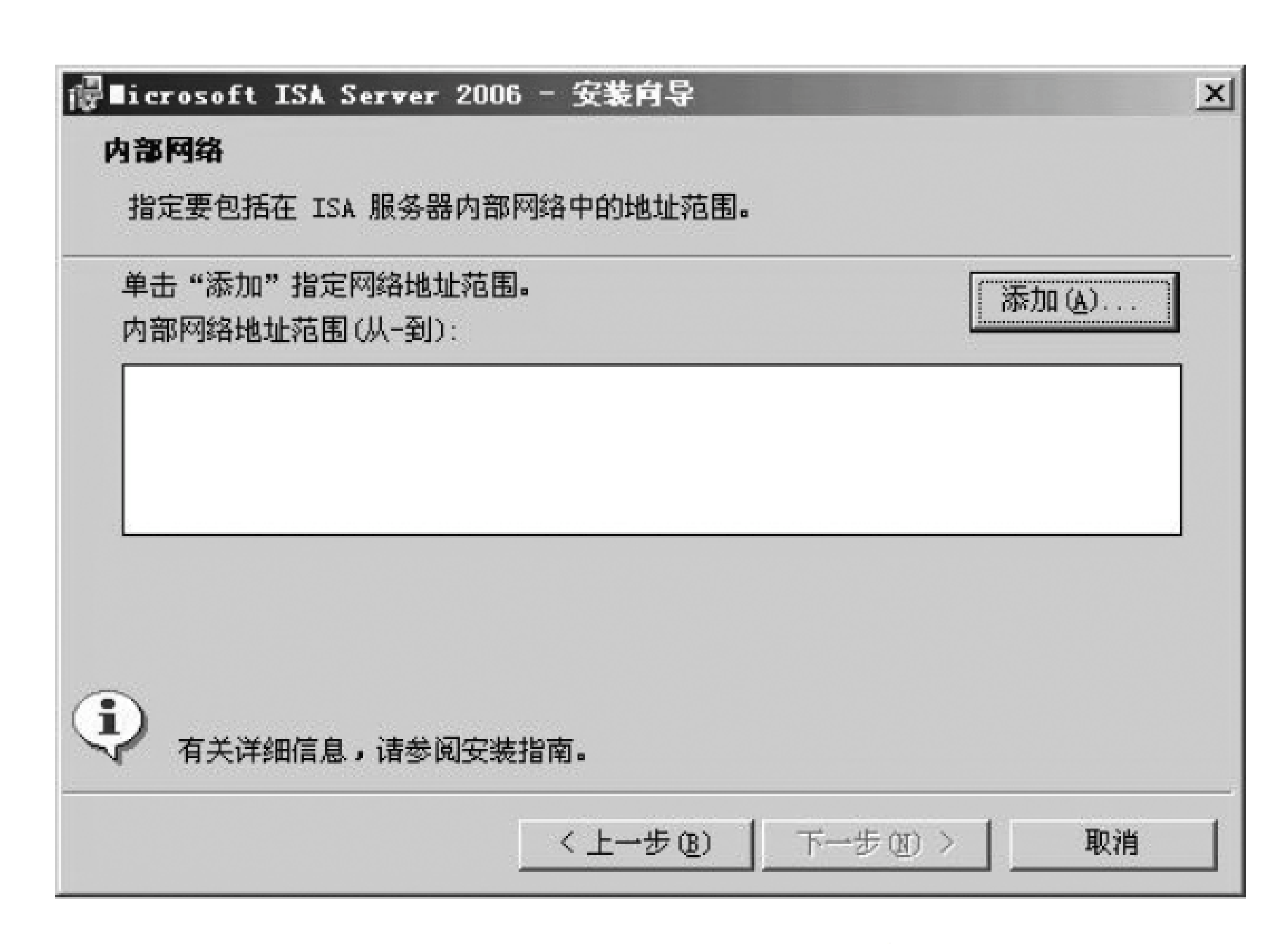


图 5-42 【内部网络】对话框



(10) 在弹出的【地址】对话框中单击【添加适配器】按钮，选择内部网络的 IP 地址范围(也可以通过【添加范围】按钮自行输入)，如图 5-43 所示。

(11) 在弹出的【选择网络适配器】对话框中选中内部网络的网卡(内网卡)后单击【确定】按钮，将此网卡所连接的网络设置为内部网络(IP 地址 192.168.2.0—192.168.2.255)，如图 5-44 所示。

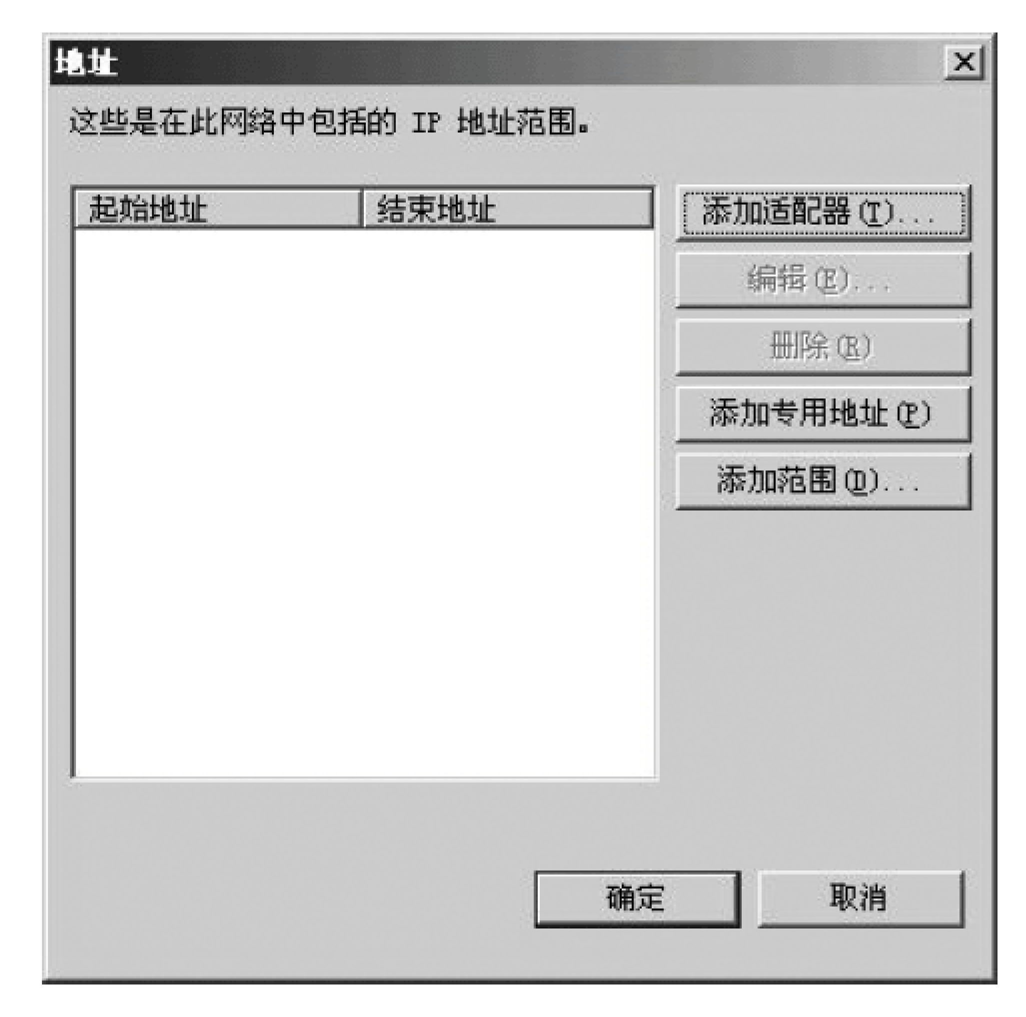



图 5-43 【地址】对话框



图 5-44 【选择网络适配器】对话框

(12) 在【地址】对话框中单击【确定】按钮，在【内部网络】对话框中单击【下一步】按钮。

(13) 在【防火墙客户端连接】对话框中单击【下一步】按钮。在此对话框中选择是否允许旧版的防火墙客户端采用非加密的方式来连接 ISA Server 防火墙，默认是不允许的。

(14) 在出现的【服务警告】对话框中单击【下一步】按钮。

(15) 在出现的【可以安装程序了】对话框中单击【安装】按钮。

(16) 在出现的【安装向导完成】对话框中直接单击【完成】按钮。

5.4.3 测试 ISA Server 防火墙是否安装成功

选择【开始】/【所有程序】/Microsoft ISA Server/【ISA 服务器管理】选项，内建的默认规则会拒绝所有的流量，如图 5-45 所示，故 ISA Server 计算机自己要访问外部资源时会被拒绝。这里将利用 ISA Server 2006 计算机来测试是否可以访问外部网页，至于访问规则的其他详细说明将在后面部分说明。

图中企业名称默认为“企业”，而阵列名默认就是 ISA Server 2006 的计算机名称 ISA2006，刚才所说的默认规则就是定义在企业规则内，这个规则会被应用到 ISA2006 阵列内，而且其应用顺序是在阵列防火墙之后。由于测试环境中只有单一阵列、单一服务器，因此为了便于学习起见，以后将只建立阵列防火墙原则内的访问规则。

技巧： 通过右击图 5-45 中阵列名 ISA2006 并选择【导出】命令，将 ISA Server 2006 的原始设置备份起来，以便将来随时可通过右击阵列名 ISA2006 并选择【导入】命令的方法将 ISA Server 2006 的设置还原到原始设置值。





图 5-45　【ISA 服务器管理】窗口

1. 被 ISA Server 防火墙阻挡的测试

(1) 将 Internet Explorer 的安全等级降为中安全性，否则默认的高安全性会阻挡连接大部分的网站。在 ISA Server 2006 计算机上选择【开始】/【控制面板】/【添加或删除程序】/【添加/删除 Windows 组件】命令，取消选中【Internet Explorer 增强的安全配置】选项，然后按向导提示并单击【确定】按钮即可。

(2) 尝试访问外部网站，此时连接外部网站的网页会被 ISA Server 防火墙阻挡，如图 5-46 所示。

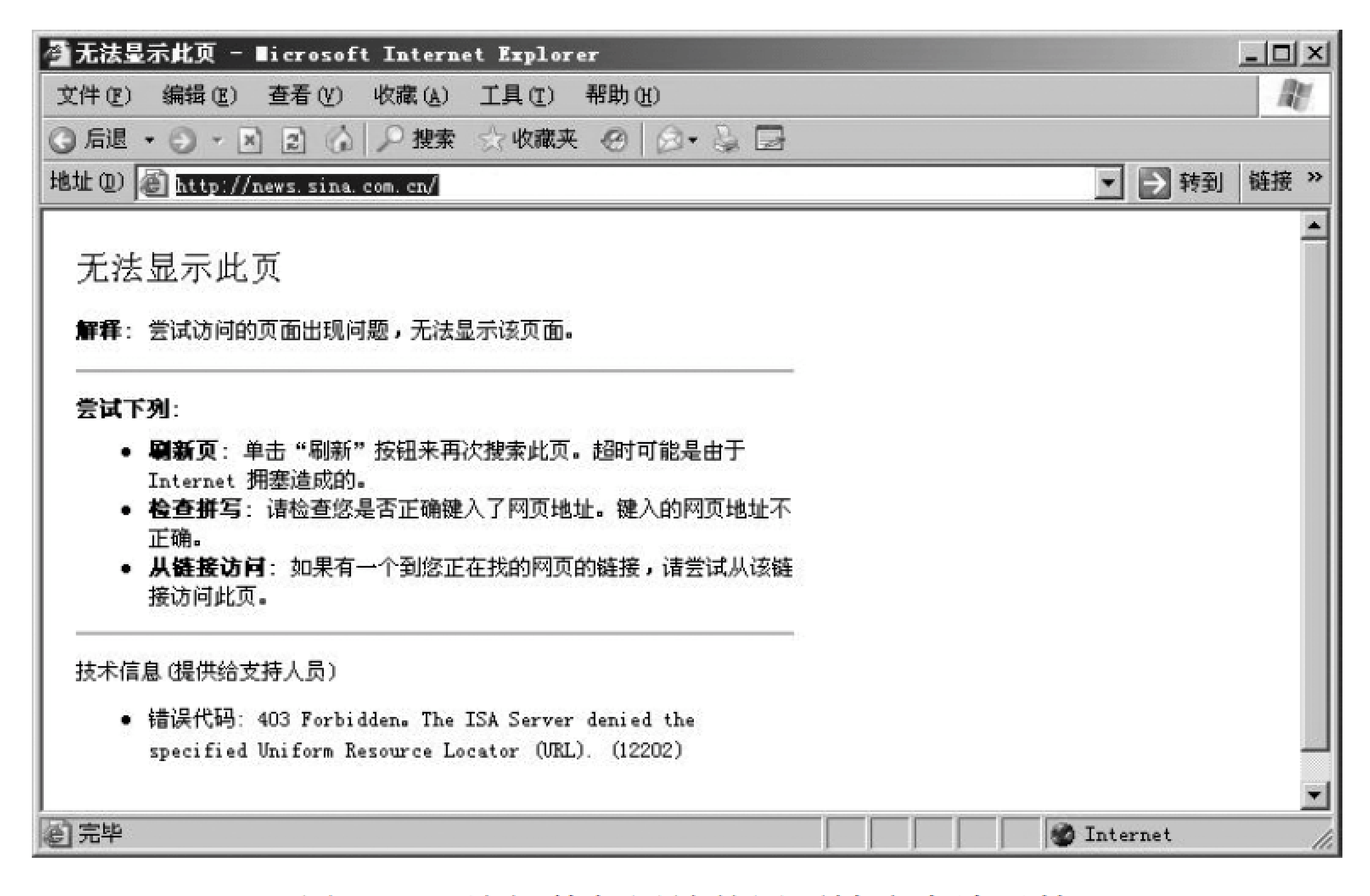


图 5-46　访问外部网站的网页被防火墙阻挡

2. 创建访问规则使开放 ISA Server 2006 计算机可以上网

方法如下：

(1) 在【ISA 服务器管理】窗口左侧列表框中单击【防火墙策略】，再单击右边【任务】选



项卡的【创建访问规则】选项。

（2）在【欢迎使用新建访问规则向导】对话框中为此访问规则命名（例如“允许本机主机访问外部网站”）。在【规则操作】对话框选择【允许】单选按钮，允许本机主机访问外部网站，如图 5-47 所示。单击【下一步】按钮。

（3）选择规则要应用到的协议为“所选的协议”，单击【添加】按钮，表示只开放连接网站的协议，如图 5-48 所示。

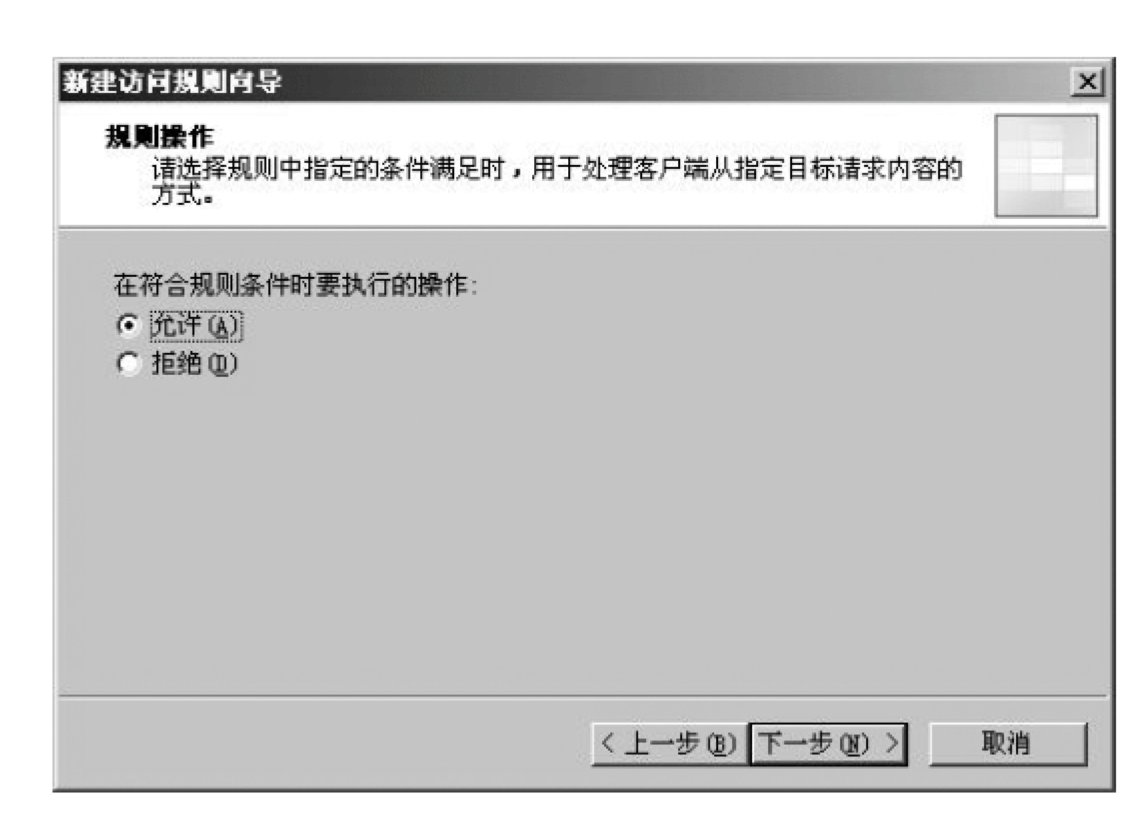


图 5-47 【规则操作】对话框



图 5-48 【协议】对话框

（4）在图 5-49 中依次选择并添加 HTTP、HTTPS，单击【关闭】按钮。

（5）单击【下一步】按钮，如图 5-50 所示。



图 5-49 【添加协议】对话框



图 5-50 添加协议后的【协议】对话框

（6）在【访问规则源】对话框中选择此规则的应用来源，在此，只想让 ISA Server 2006 计算机本身可以上网，因此单击【添加】按钮，在【添加网络实体】对话框中选择【本地主机】并单击【添加】按钮，再单击【访问规则源】对话框的【下一步】按钮，如图 5-51 所示。

（7）将此规则的应用目的地设置为“外部”，也就是允许访问外部所有的网站，如图 5-52 所示。





图 5-51　添加网络到【访问规则源】



图 5-52　添加网络到【访问规则目标】

（8）在【用户集】对话框中单击【下一步】按钮，以便将此原则应用到所有的用户，如图 5-53 所示。



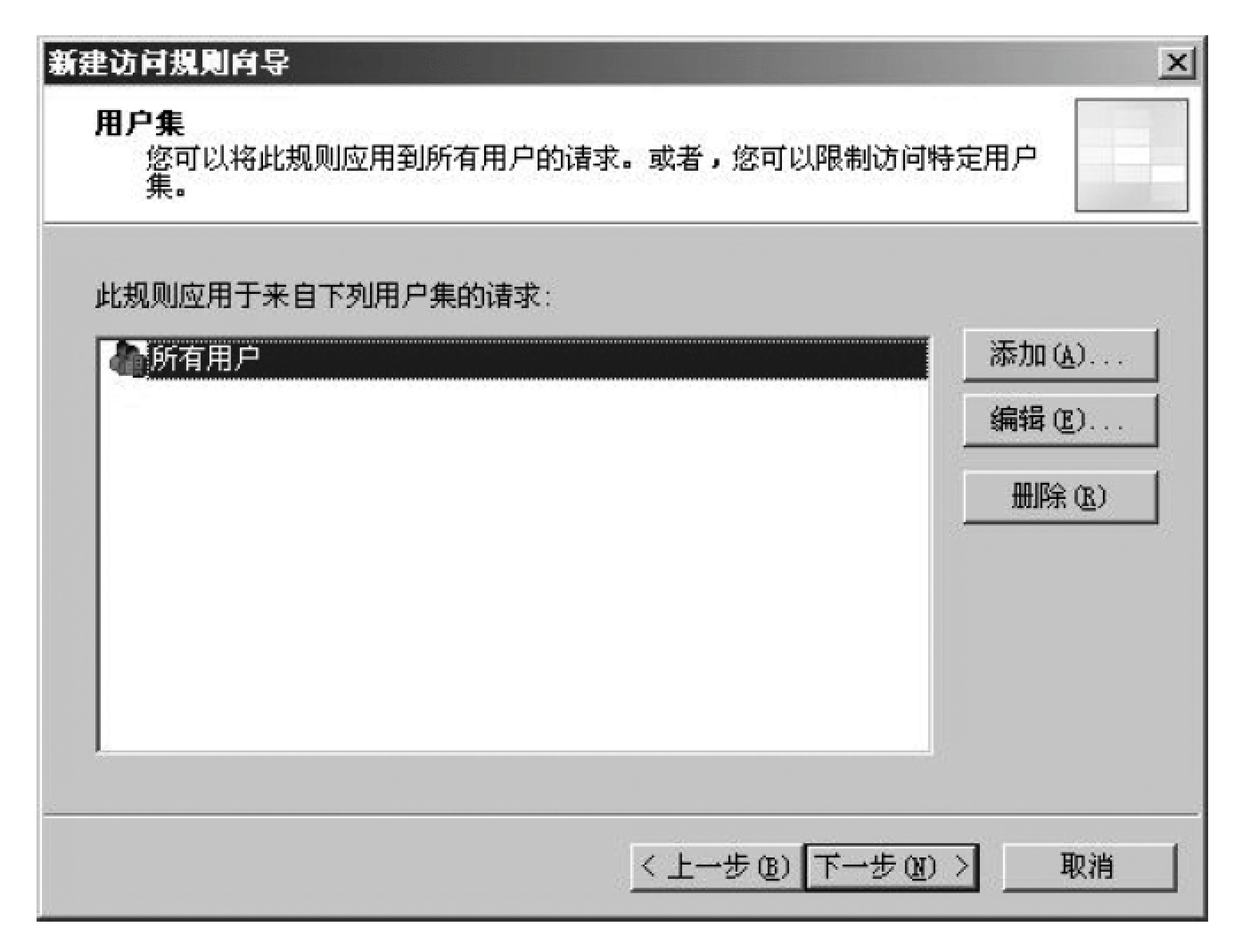


图 5-53 【用户集】对话框

(9) 在【完成新建访问规则向导】对话框中单击【完成】按钮；在【防火墙策略】配置窗口中单击【应用】按钮，如图 5-54 所示。



图 5-54 应用新建的访问规则

(10) 完成设置后，这些配置会保存到存储服务器(CSS)内，ISA Server 会定期(默认为 15 秒)检查与应用 CSS 内的最新更新(在此实验中 ISA Server 与 CSS 是同一台计算机)，并保持与 CSS 同步，如图 5-55 所示。

(11) 打开浏览器测试 ISA Server 2006 计算机是否能上网。

5.5 ISA 防火墙策略

仅有了网络规则(网络之间关系规则)还是不够的，还必须为各种应用配置防火墙策略，只有这样才能确保受保护的网络的安全。ISA 防火墙策略主要包括访问规则和发布规则，







图 5-55 ISA Server 与 CSS 同步

是 ISA Server 的核心所在，也是 ISA 防火墙应用的难点所在。

5.5.1 ISA 防火墙策略工作方式

用 ISA Server 可以创建包含一组访问规则和发布规则的防火墙策略。这些规则与网络规则一起，共同决定了客户端如何跨网络来访问资源。

1. 传出请求

ISA Server 的一个主要功能是连接源网络与目标网络，同时阻止恶意访问。为了帮助建立此连接，用户可使用 ISA Server 来创建允许源网络中的客户端，访问目标网络中的特定计算机的访问策略。此访问策略决定了客户端如何访问其他网络。

当 ISA Server 处理传出请求时，它检查网络规则和防火墙策略规则以确定是否允许访问。可以配置某些规则应用于特定的客户端。在这种情况下，可以通过 IP 地址或用户名来指定客户端。ISA Server 根据请求对象的客户端类型以及 ISA Server 的配置来相应的处理请求。

首先，ISA Server 检查网络规则，以确认两个网络已连接。如果网络规则定义了源网络与目标网络之间的连接，ISA Server 将处理访问策略规则。

其次，ISA Server 按顺序检查访问规则。如果对该请求应用了允许规则，ISA Server 将允许该请求。特别是在请求与下列规则条件相匹配时，ISA Server 将应用下列规则。

- 协议。
- 从(源)地址和端口。
- 计划。
- 到(目标)地址、名称、URL。
- 用户。
- 内容组。

应用规则之后，ISA Server 不再请求与其他任何规则相匹配，并停止规则评估。随后，



ISA Server 实际上可能拒绝请求，具体情况取决于应用于规则的其他协议筛选。

最后，ISA Server 再次检查网络规则，以确定网络是如何连接的。ISA Server 检查 Web 链规则（请求对象是 Web 代理客户端）或防火墙链配置（请求对象是 SecureNAT 或防火墙客户端），以确定将如何处理请求。

例如，假定用户将 ISA Server 安装到具有两个网卡的计算机上：一个网卡连接到外部网络（例如 Internet），另一个则连接到内部网络。公司的许可原则是允许所有用户访问所有站点。在这种情况下，用户策略应包含下列访问策略规则。

- 在源网络（内部网络）与目标网络（外部网络，例如 Internet）之间建立连接的网络规则。
- 允许所有内部网络的客户端在任何时候使用任何协议访问 Internet 任何站点的访问规则。

2. 传入请求

ISA Server 可以使服务器安全地接受来自其他网络客户端的访问。使用 ISA Server 创建一条发布策略以便安全地发布服务器。发布策略包含 Web 发布规则、服务器发布规则、安全 Web 发布规则以及邮件服务器发布规则，它与 Web 链规则一起共同确定如何访问发布的服务器。

可以使用下列 ISA Server 规则之一来发布服务器。

- Web 发布规则：发布 Web 服务器内容。
- 服务器发布规则：发布非 Web 服务器内容。
- 安全 Web 发布服务器：发布安全套接字层（SSL）内容。

当 ISA Server 处理来自客户端的 HTTP 或 HTTPS 请求时，它检查发布规则和 Web 链规则，以确定是否允许该请求，以及将由哪一台服务器来处理该请求。

对于非 HTTP 请求，ISA Server 检查网络规则，然后检查发布规则以确定是否允许该请求。对于传入的 Web 请求，是按下列顺序来处理规则的：

- Web 发布规则。
- Web 链规则。

例如，有这样一个方案：将 ISA Server 安装到具有两个网络适配器的计算机上，其中一个适配器连接到 Internet，而另一个则连接到内部网络，将应用下列规则。

- 如果 Web 发布规则明确地拒绝请求，该请求将被拒绝。
- 如果 Web 链规则规定请求应由路由到特定的上游服务器或备用的主持站点，将由指定的服务器处理该请求。
- 如果 Web 链规则规定请求应由路由到指定的服务器，将由内部 Web 服务器返回对象。

5.5.2 防火墙访问规则

访问规则决定源网络上的客户端如何访问目标网络上的资源。

可以将访问规则配置为适用于所有 IP 通信、适用于特定的协议定义集，或适用于除所选协议之外的所有 IP 通信。如图 5-56 所示，在中间【防火墙策略】选项卡里列出来的是用户创建

的访问规则，用户可以单击右边【任务】选项卡的【创建访问规则】选项创建新的访问规则。



图 5-56　防火墙访问规则

1. 通信规则

ISA Server 包含预配置的、已知协议定义的列表，其中包括最广泛使用的 Internet 协议。用户还可以添加或修改其他协议。当客户端使用特定协议请求对象时，ISA Server 将检查访问规则。仅当某个访问规则明确允许客户端使用特定的协议进行通信，并且允许访问请求的对象时才处理请求。

2. 访问规则和应用程序筛选器

一些应用程序筛选器将创建和安装新协议定义。禁用应用程序筛选器之后，同时将禁用其所有协议定义，也就是说将阻止使用该协议定义的通信。例如，如果禁用流媒体筛选器，则使用 Windows Media 和 RealNetworks 协议定义的所有通信都将被阻止。其他应用程序筛选器用于处理现有协议定义，这些协议定义既可以是用户定义的，也可以是通过 ISA Server 配置的。禁用这些应用程序筛选器之后，不会禁用它们筛选的协议定义。例如，即使禁用简单邮件传输协议(SMTP)筛选器，可能仍然允许传递未筛选的 SMTP 协议定义。

当访问规则允许所有 IP 通信时，ISA Server 将任何匹配该规则的通信传递到适合的应用程序筛选器。如果通信不符合应用程序筛选器的标准，ISA Server 将拒绝通信，并且将关闭连接。

当由应用程序筛选器定义协议或将访问规则适用于只有一个首要连接的协议时(例如，超文本传输协议(HTTP))，访问规则将适用于防火墙客户端和 SecureNAT 客户端。

如果协议拥有辅助连接，并且它不是由应用程序筛选器定义的，则访问规则只适用于首要连接。也就是说，如果应用程序使用拥有辅助连接的协议，则此应用程序将只在防火墙客户端上运行。



对于 SecureNAT 客户端，如果将访问规则配置为应用于所有 IP 通信，则该规则将只应用于所有定义的协议。

3. 每条规则筛选

应用程序筛选将基于每条规则进行应用，这意味着可以选择最适合于特定的安全需求的防火墙策略。例如，假设允许所有内部用户使用所有协议访问 Internet，在这种情况下，可以选择启用最大筛选。然而，假设还要允许从内部网络到特定的受信任网络进行较低限制的远程过程调用(RPC)访问。在这种情况下，可能要考虑不应用 RPC 筛选器严格的符合标准(采用该方式将允许网络之间进行 DCOM 通信)。

每条规则筛选可用于下列应用程序筛选器中的访问规则。

- HTTP 筛选器。
- RPC 筛选器。

4. 默认规则

在安装 ISA Server 时将创建一条默认规则，用于拒绝出入所有网络的全部访问。不能修改或删除此默认规则。

> **注意：** 由于 ISA Server 首先处理系统策略规则，因此允许本地主机访问外部网络的系统策略规则，将替代特别配置用于拒绝这种访问的所有访问策略规则。

5.5.3 ISA 防火墙发布规则

在 ISA Server 中，访问规则和发布规则是非常重要的应用规则。访问规则确保了受保护的网络资源不被非法访问和使用；而发布规则就确保了各种应用服务器时刻处于严格的保护状态，通过规则来过滤非法的访问与使用。

1. ISA 防火墙 Web 发布规则

ISA Server 使用 Web 发布规则来缓解与发布 Web 内容有关的问题，同时又不危及网络的安全性。Web 发布规则决定了 ISA Server 将如何拦截对 Web 服务器上的超文本传输协议(HTTP)对象的传入请求，以及 ISA Server 将如何代表 Web 服务器进行响应。当请求被转发到位于 ISA Server 计算机后面的 Web 服务器时，如果可能，将从 ISA Server 缓存中提供所请求的对象。

Web 发布规则本质上是将传入请求与相应的 Web 服务器匹配。Web 发布规则还可以配置高级筛选功能，从而既发布基于 Web 的信息，又防止其受到恶意的访问。也要注意，新规则仅适用于新连接。

配置 Web 发布规则时，除了可以访问已发布的 Web 服务器的用户或计算机，还应指定下列设置。

- Web 服务器的名称(或 IP 地址)：可以限定规则适用于服务器上的所有网站，还有特定的网站。

- 路径映射：转发请求之前，ISA Server 可以修改请求中指定的外部路径，并将其映射为相应的内部路径。
- 源：可以访问已发布的 Web 服务器的网络对象。请注意指定的网络对象还必须包含在为此 Web 发布规则指定的 Web 侦听器中。
- Web 侦听器：这是 ISA Server 计算机上侦听来自客户端的请求的 IP 地址。
- 桥接：使用桥接可以配置 HTTP 请求如何转发到已发布的服务器。
- 链接转换：使用链接转换，可以配置 ISA Server 如何扫描网页中的链接，并使用外部名称和路径来对其进行更新。

可以通过配置 HTTP 筛选来进一步筛选向 Web 服务器发出的请求。

注意：建议不要在 ISA Server 发布的 Web 服务器上启用目录浏览。此外，Web 服务器不能要求摘要式身份验证或基本身份验证，否则，Web 服务器的内部名称或 IP 地址可能会在 Internet 上暴露。

(1) 操作。Web 发布规则指定将由哪一台服务器(如果有)返回所请求的对象。请求可能被丢弃，也可能被重定向到另一个站点，并且通常重定向到公司网络中的 Web 服务器。

当配置将请求重定向到主持站点的规则时，ISA Server 从主机上的路径(在请求中指定)中检索对象。例如，假定指定 ISA Server 将对 example. microsoft. com/development 的请求转发到名为 Dev 的主机。那么，当客户端请求 example. microsoft. com/development 中的对象时，ISA Server 将从 Dev 上的 development 文件夹中检索对象。

Web 发布规则通过阅读主机头来确定所请求的目标。

(2) 路径映射。在将请求转发到发布的 Web 服务器之前，ISA Server 会检查请求中所指定的(外部)路径。如果配置路径映射，ISA Server 将用相应的路径名来替换请求中所指定的路径。应注意指定的每个路径必须是确定而且唯一的。

指定路径映射时应遵循下列准则。

- 指定请求将映射到的内部路径时，使用格式：/mypath/ * 。
- 不能在路径中使用通配符。例如，不要指定 mypath * /或/mypath * 。
- 配置路径映射时，应避免指定文件名。否则，可能将仅处理路径完全匹配的请求。

(3) 桥接。创建 Web 发布规则时，可以进一步保护 HTTP 通信的安全性。即便最初的通信使用的是 HTTP，在 ISA Server 收到请求后，也可以使用 SSL 重定向通信。如果请求被作为 SSL 请求重定向，则会加密数据包。这种重定向被称为桥接。

可以设置 HTTP 或 SSL 请求，并将被作为 FTP 请求传递到 Web 服务器。如果外部客户端使用 HTTP 或 SSL 请求对象，那么 ISA Server 可以使用 FTP 将请求重定向到内部 Web 服务器。如果以这种方式配置桥接，可以指定在桥接 FTP 请求时将使用哪个端口。

上游 Web 服务器可能要求客户端证书，在这种情况下，应配置 ISA Server 使用特定的客户端证书进行身份验证。

如果配置 Web 发布规则要求安全通道，则对指定目标的所有客户端请求都必须使用为 SSL 连接指定的端口。

(4) 发布具有相同域名的网站。客户端通过 ISA Server 发布完全限定的域名(FQDN)来识别发布的网站，这意味着网站的 FQDN 就是在 Web 发布规则中配置的 FQDN。通过



使用同一个 FQDN 来发布多个 Web 服务器，客户端假定发布的两个站点实际是相同的。也就是说，Web 客户端可以将原定发往一个 Web 服务器的信息发送到另一个 Web 服务器。

（5）规则顺序。Web 发布规则是与所有防火墙策略规则一起处理的。针对每个传入的 Web 请求按顺序对它们进行处理。如果规则与请求匹配，则将相应的路由并缓存请求；如果没有与该请求匹配的规则，则 ISA Server 将处理默认规则并丢弃请求。

2．ISA 防火墙的安全 Web 发布规则

使用 ISA Server，可以创建安全 Web 发布规则，以发布用于宿主 HTTPS 内容的网站。安全 Web 发布规则确定 ISA Server 如何侦听内部 Web 服务器上的 HTTPS 对象的传入请求，以及 ISA Server 如何代表 Web 服务器进行响应。请求将转发给位于 ISA Server 计算机后面的内部 Web 服务器。注意，新规则也仅适用于新连接。

（1）桥接。使用桥接，可以配置通信传递到 Web 服务器的方式。例如，假设客户端使用安全套接字层（SSL）与 ISA Server 计算机进行通信，并且 Web 发布规则将请求映射到内部 Web 服务器，初始通信将使用 SSL。但是，默认情况下，所有后续的通信都使用不安全的协议，如 HTTP。

当创建安全 Web 发布规则时，可以配置 SSL 请求如何被重定向为 HTTP 请求或 SSL 请求。如果请求被重定向为 SSL 请求，那么 ISA Server 将重新加密数据包，然后再将其传递到 Web 服务器，这样便建立了与 SSL Web 服务器进行通信的新的安全通道。这种重定向也称为 SSL 桥接。

（2）隧道。当配置安全 Web 发布规则以使用隧道模式时，ISA Server 将未修改的、经过加密的通信转发到已发布的 Web 服务器。也就是说，ISA Server 不对通信执行任何其他筛选。

使用隧道模式（与桥接模式相对）的安全 Web 发布规则与 Web 发布规则相比，更类似于服务器发布规则。许多 Web 发布功能（包括链接转换和路径映射）不适用于这些规则，此规则不能应用于特定用户（只应用于网络对象）。

（3）侦听器。当配置安全 Web 发布规则时，定义的是如何访问已发布的 Web 服务器上的 HTTPS 内容。应该为安全 Web 发布规则指定适当的侦听器，将其配置为在某个 HTTPS 端口上进行侦听。

3．服务器发布规则

ISA Server 使用服务器发布来处理内部服务器的传入请求，如文件传输协议（FTP）服务器、结构化查询语言（SQL）服务器等，请求被转发到下游位于 ISA Server 计算机后面的内部服务器。

（1）服务器发布概述。服务器发布实际上允许内部网络上的任何计算机发布到 Internet。由于所有传入请求和传出响应都要通过 ISA Server，因此这样并不会危及安全性。当由 ISA Server 计算机发布服务器时，发布的 IP 地址实际上是 ISA Server 计算机的 IP 地址。请求对象的用户认为它们是在与 ISA Server（其名称或 IP 地址在用户请求对象时被指定）进行通信，实际上它们是请求发布服务器中的信息。当从访问发布服务器的客户端所在的网络，到发布的服务器所在的网络这个方向上存在网络地址转换（NAT）关系时也

是如此。在配置路由的网络关系时，客户端使用发布服务器的实际 IP 地址来访问它。

服务器发布规则决定服务器发布的执行方式，本质上是筛选通过 ISA Server 计算机的所有传入和传出请求。服务器发布规则将传入请求映射到 ISA Server 计算机后面的相应服务器。这些规则将按照指定，动态授予从 Internet 用户到特定发布服务器的访问权限。

发布的服务器是 Secure NAT 客户端。因此，在 ISA Server 计算机上创建服务器发布规则之后，不需要发布服务器的特殊配置。应注意，ISA Server 必须被配置为发布的服务器上的默认网关。

注意： 不支持发布 IP 等级和 Internet 控制消息协议(ICMP)的首要协议，一个例外情况是点对点隧道协议(PPTP)。该协议是 TCP 连接和一般路由封装(GRE)数据包的组合，并且受支持。同样，新规则仅适用于新连接。服务器发布规则适用于一个协议。

(2) 每条规则筛选。应用程序筛选将基于每条规则进行应用，这意味着用户可以选择最适合于特定安全需求的防火墙策略，每条规则筛选可用于 Exchange RPC 筛选器的服务器发布规则。

(3) 改写默认端口。使用 ISA Server 发布服务器时，默认情况下防火墙将侦听相应协议标准端口上的传入请求，并且将传入连接传递到发布服务器上的相同标准端口。例如，在发布 FTP 服务器时，ISA Server 将侦听端口 21(与 FTP 协议相关联的端口)上的传入请求，并将传入连接传递到发布的服务器上的端口 21。通过在发布规则中指定其他端口，可以改写标准端口。

注意： 在发布网络之间存在路由网络关系的远程过程调用(RPC)接口时，将忽略端口改写。发布规则将使用原始 IP 地址和端口。

(4) 服务器发布的工作方式。ISA Server 在服务器发布过程中执行下列步骤：

① Internet 的客户端计算机被认为是发布服务器的 IP 地址请求对象。IP 地址实际上与 ISA Server 计算机相关联，这是属于 ISA Server 计算机的外部网络适配器的 IP 地址。

② ISA Server 计算机处理请求，将 IP 地址映射到内部服务器的内部 IP 地址。

③ 内部服务器将对象返回到 ISA Server 计算机，通过它将对象传递到发出请求的客户端。

(5) 服务器发布规则的用法。在很多情况下，实际上可以使用访问规则(而不是服务器发布规则)使服务器可用于客户端。需要考虑的问题如下：

- 从发布的服务器网络到客户端网络存在 NAT 网络关系时，必须使用服务器发布规则。
- 一个服务器发布规则只能发布一个标识的服务器。要发布多个服务器，需要多个规则。
- 使用服务器发布规则，可以配置端口改写。

(6) 发布 DNS 服务器。ISA Server 并不转换 DNS 服务器的 IP 地址。要发布 DNS 服务器，请在本地主机网络和包含 DNS 服务器的网络之间配置路由的网络关系。同样，ISA Server 必须知道 DNS 服务器的 IP 地址。



(7) 禁用规则。禁用服务器发布规则之后，将拒绝任何尝试连接到服务器的请求。但是应注意，ISA Server 不关闭活动连接。

5.6 ISA Server 的网页缓存

5.6.1 网页缓存概述

ISA Server 通过缓存(Cache)功能来加快内部网络访问外部网页与 FTP 服务器的速度，也可以加快外部用户访问内部网页与 FTP 服务器的速度。

ISA Server 将用户较常访问的网页保存到缓存区中，不但让用户更快取得所需网页，同时也可节省网络带宽、增加网络效率。ISA Server 同时利用内存(RAM)与硬盘来作为缓存对象的保存地点(缓存区)。当 ISA Server 收到用户 HTTP 或 FTP 的访问请求时，只要所需对象在缓存区中，ISA Server 便会直接从缓存区读取该对象给用户，因此用户不需要通过 Internet，就能很快取得所需的网页对象或 FTP 文件。

如果用户所请求的对象为新对象(是缓存区没有的对象)，ISA Server 便会通过 Internet 去取得对象，然后先将对象保存到内存内，并且隔一段时间后再将内存内的对象转移到硬盘内。由于内存的访问速度比硬盘快得多，因此只要某对象被访问的频率较高，ISA Server 便会尽量让它继续留在内存内，以便提高用户访问该对象的速度。

5.6.2 搭建网页缓存测试环境

按图 5-57 所示搭建网页缓存实验的测试环境。

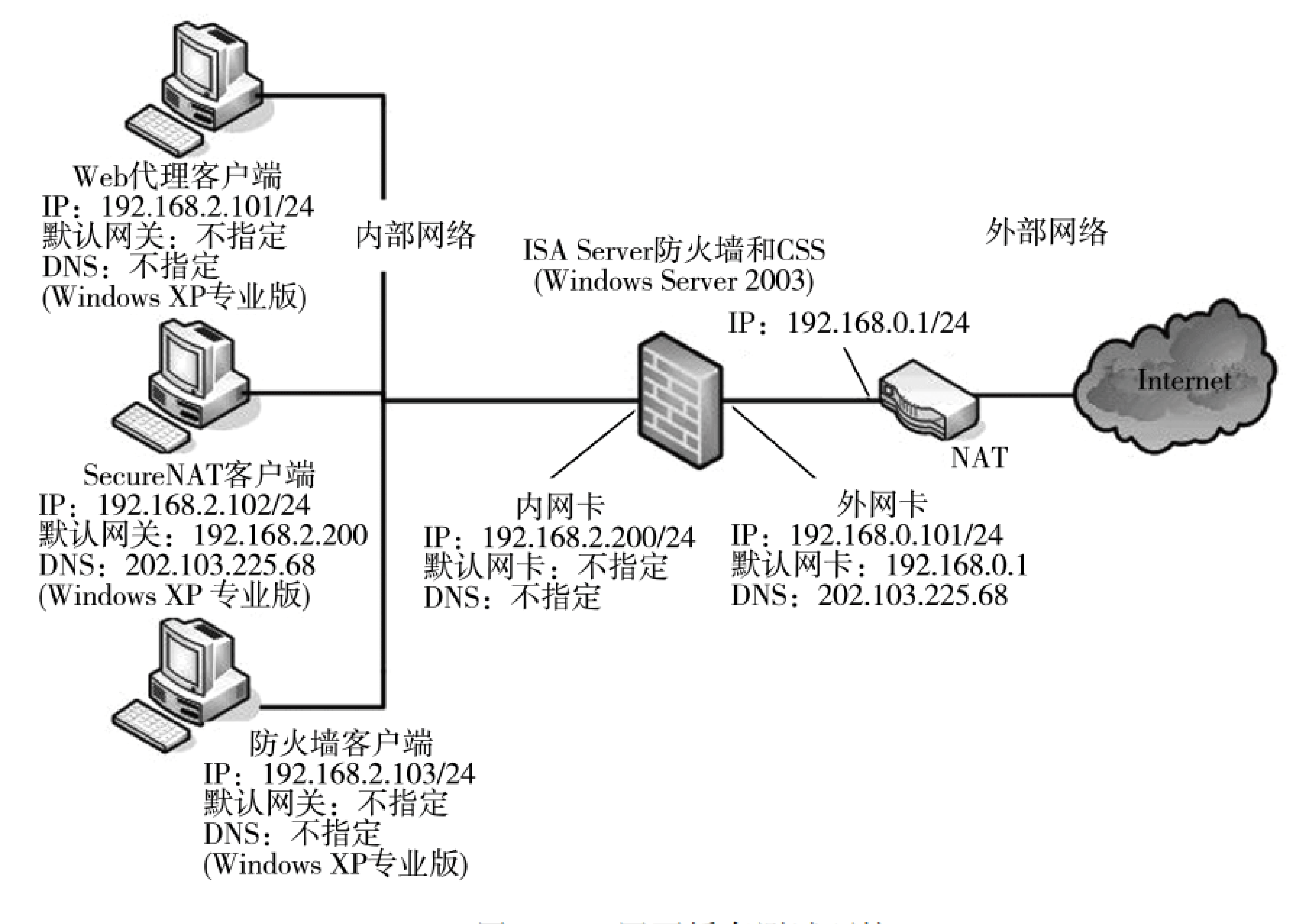


图 5-57　网页缓存测试环境



5.6.3　缓存设置

1. 缓存硬盘的大小设置

(1) 在【ISA服务器管理】窗口左侧列表中选择【配置】/【缓存】选项，然后在【缓存驱动器】选项卡下，再单击窗口右边的【任务】选项卡中的【定义缓存驱动器(启动缓存)】选项，如图5-58所示。

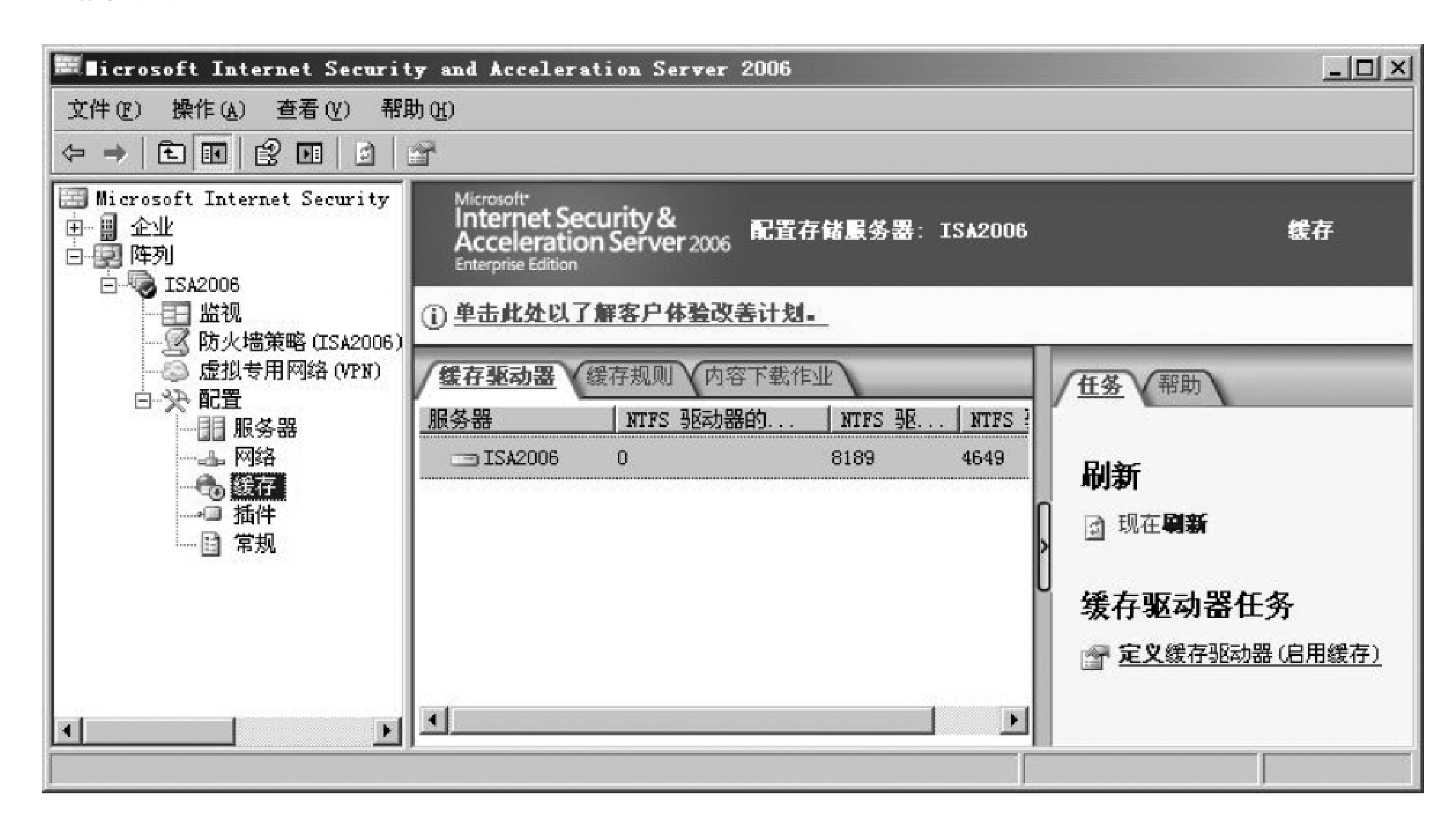


图5-58　选择【定义缓存驱动器(启动缓存)】选项

(2) 在【ISA2006属性】对话框中选择驱动器，指定此驱动器内欲被配置为缓存区的容量(比如100MB)，单击【设置】按钮，再单击【确定】按钮，如图5-59所示。



图5-59　配置缓存区的容量



（3）在【ISA 服务器管理】窗口单击【应用】按钮，如图 5-60 所示。



图 5-60 单击【应用】按钮

（4）在【ISA 服务器警告】对话框中选择【保存更改，并重启动服务】后单击【确定】按钮，如图 5-61 所示。

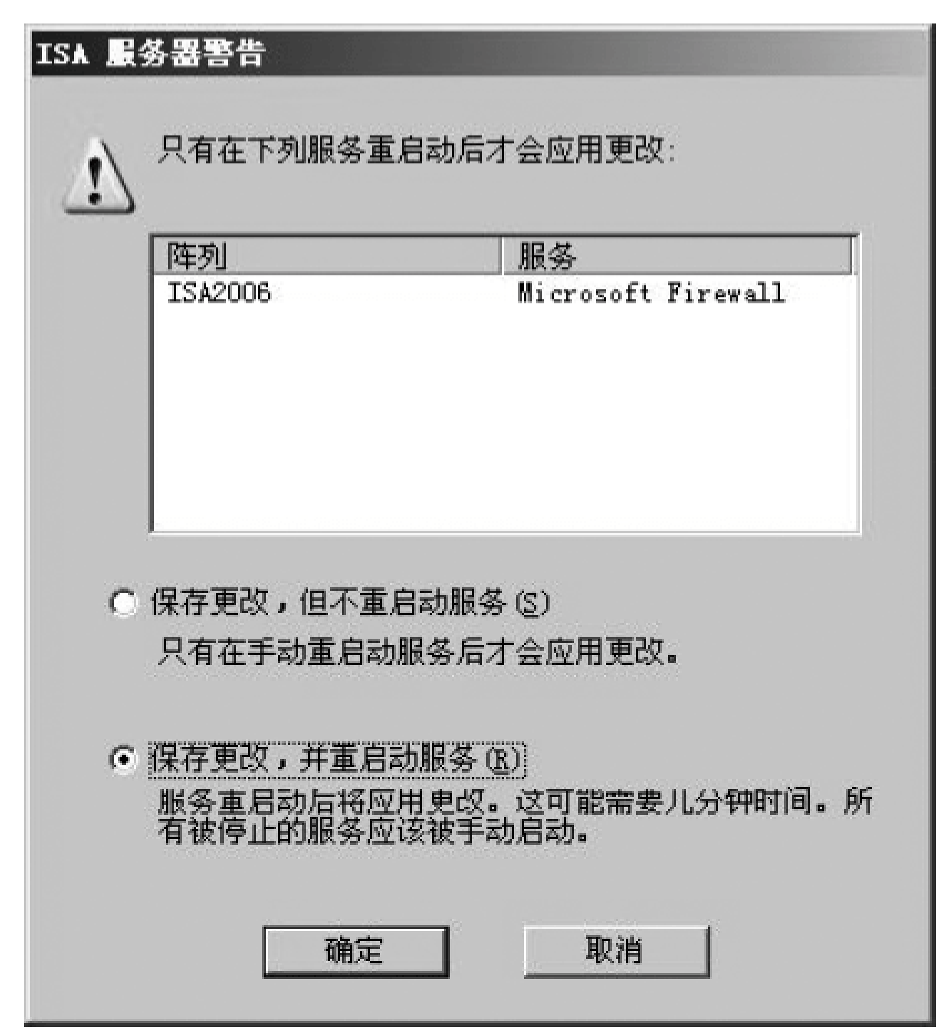


图 5-61 【ISA 服务器警告】对话框

2. 高速缓存（RAM）的大小设置

（1）在【ISA 服务器管理】窗口中选择【配置】/【缓存】选项，在【缓存规则】选项卡下，再单击窗口右边的【任务】选项卡中的【配置缓存设置】选项，如图 5-62 所示。

（2）在打开的【缓存设置】对话框中选择【高级】选项卡，在【用来缓存的可用内存百分比】文本框中设置要将可用内存中多少百分比的空间拿来作为缓存区（比如 20%），如图 5-63 所示。

（3）单击【确定】按钮。

5.6.4 设置缓存规则

通过缓存规则来决定如何缓存 Internet 的对象，例如缓存对象的有效期限、缓存哪一类的对象、如何读取缓存区的对象等。

1. 缓存规则的设置

本实验利用内置的 Microsoft Update 缓存规则来说明缓存规则的设置过程。在【ISA 服务器管理】窗口中选择【配置】/【缓存】选项，单击【缓存规则】选项卡下的【Microsoft



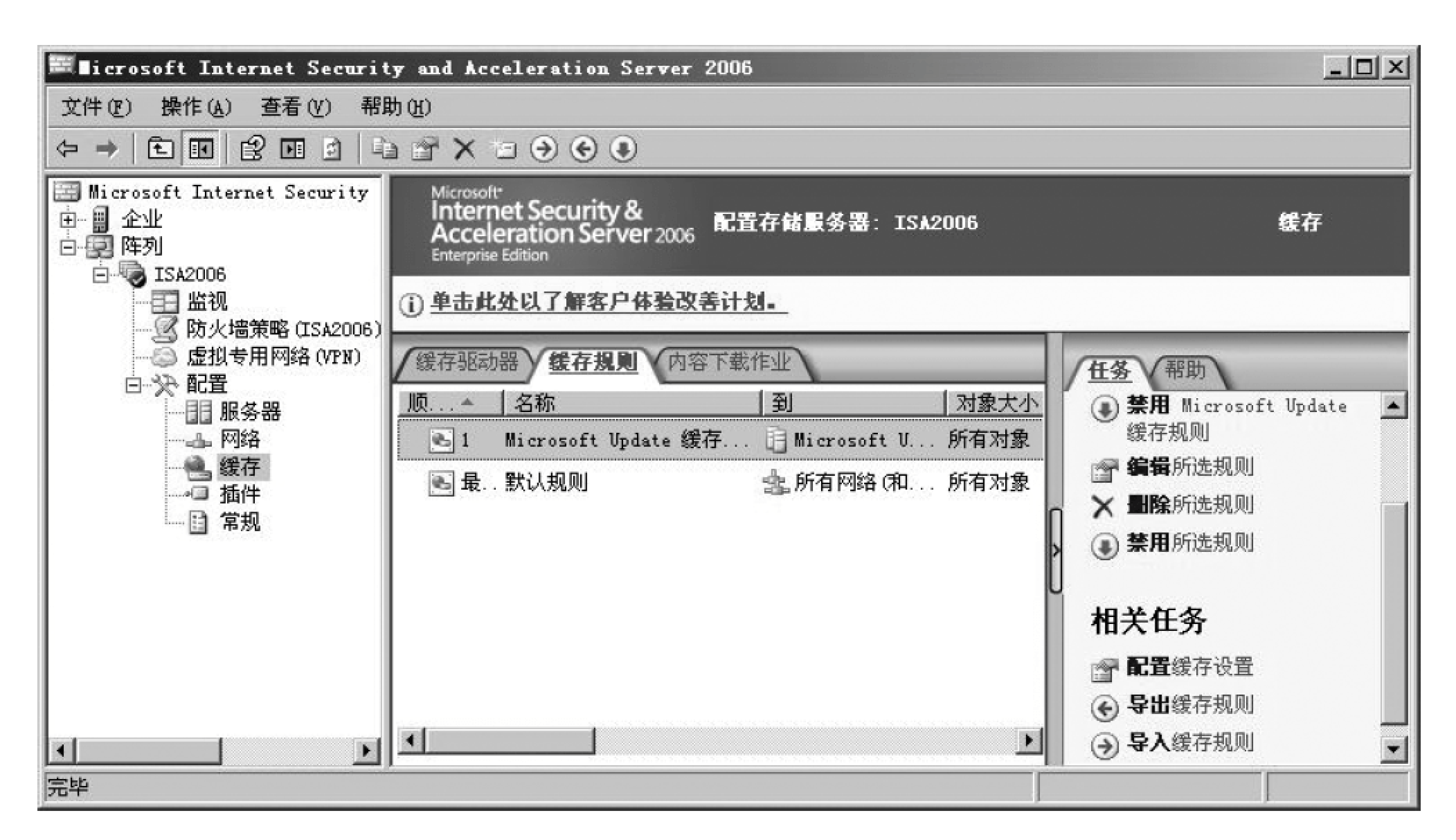


图 5-62　选择【配置缓存设置】选项

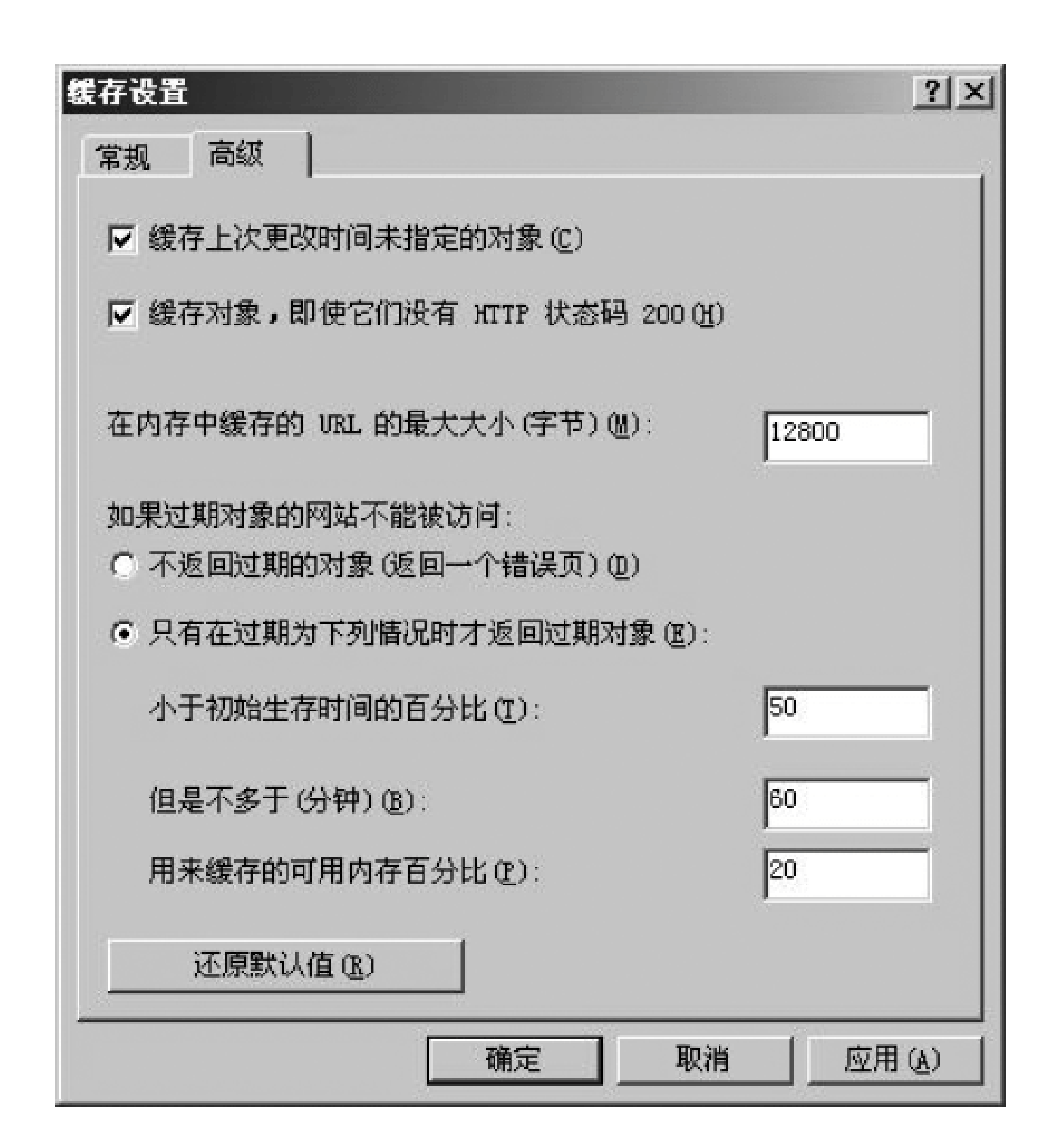


图 5-63　缓存设置的【高级】选项卡

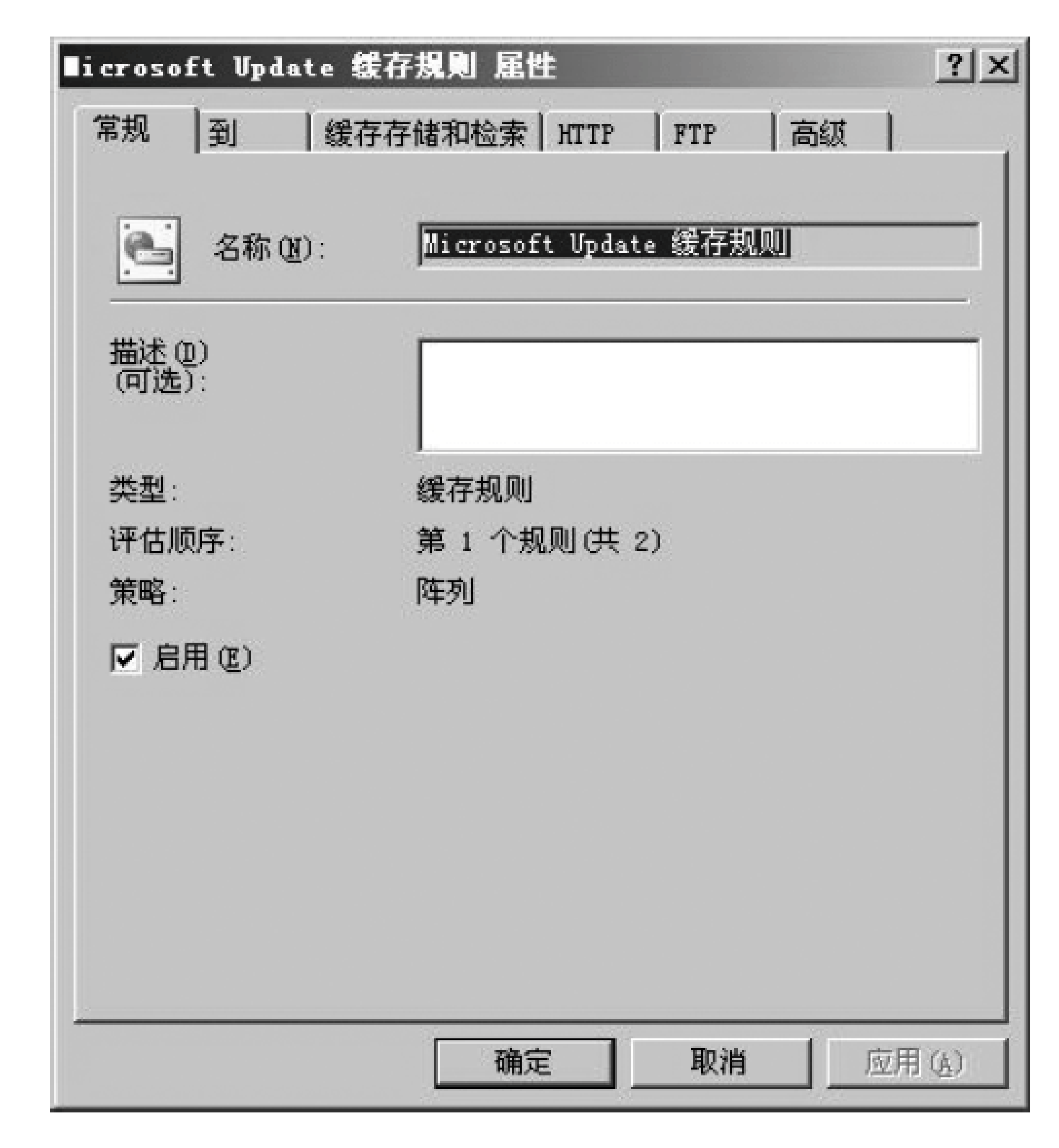
Update 缓存规则】选项，再单击窗口右边【任务】选项卡中的【编辑所选规则】选项，如图 5-64 所示。

- 启用或停用规则，如图 5-65 所示，通过【常规】选项卡来选择是否启用此规则。
- 应用此规则的目标，如图 5-66 所示，通过【到】选项卡来设置此规则所应用的目标。也就是只有当用户要连接这些目标时，才会按这个规则来处理用户的请求。
- HTTP 的缓存设置，如图 5-67 所示，通过 HTTP 选项卡来启用或停用 HTTP 缓存、设置 TTL(Time to Live)等。当 ISA Server 缓存 Internet 的网页对象后，这些对象在缓存区有一定的有效期限，这个有效期限被称为 TTL。





图 5-64　选择【编辑所选规则】命令



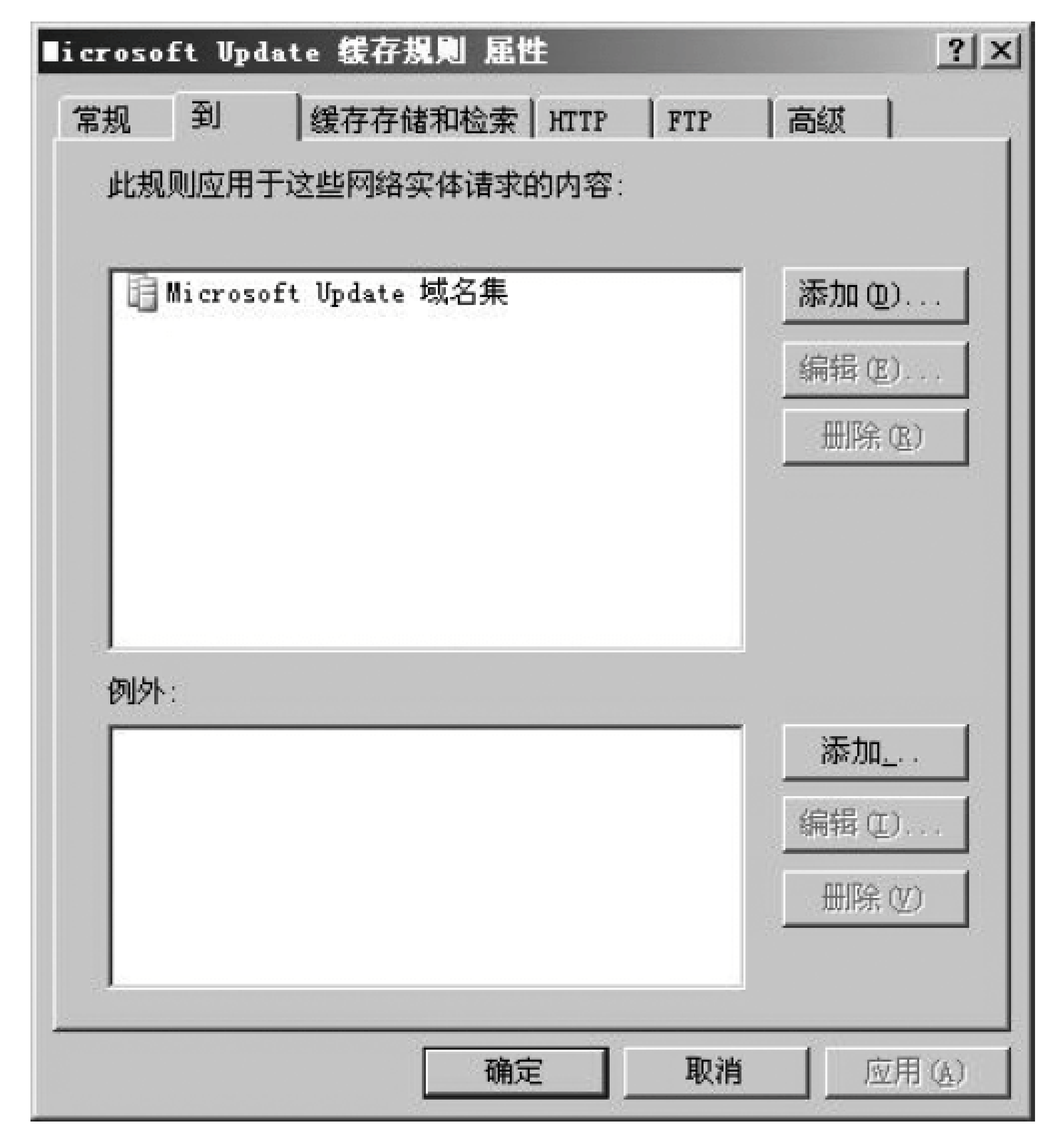




图 5-65　【常规】选项卡　　　　图 5-66　【到】选项卡

提示：网页对象的有效期限是如何决定的呢？这可从两方面考虑。

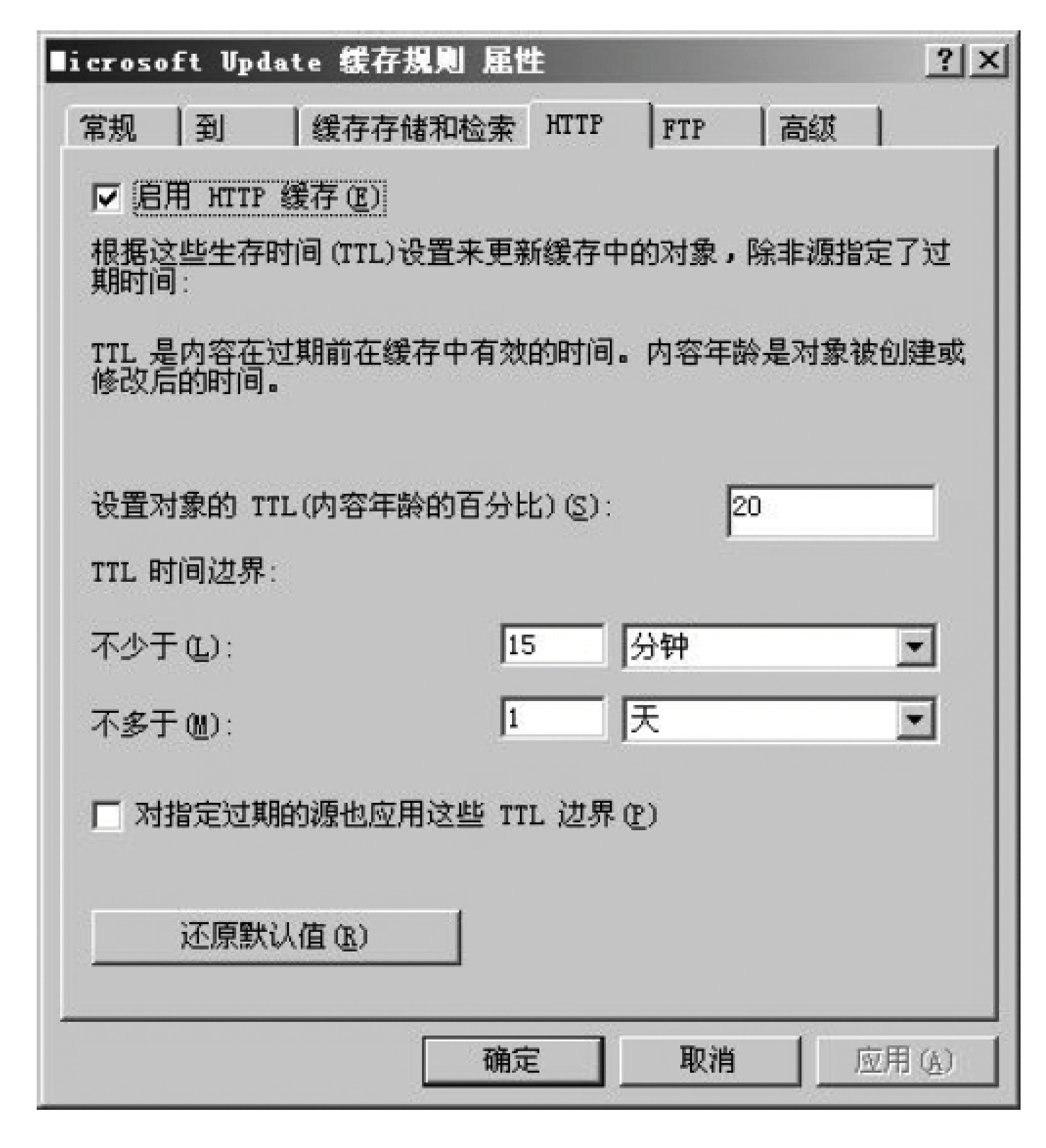
(1) 网站已经指定了该网页对象的有效期限，则该对象的有效期限默认就是指定的期限。

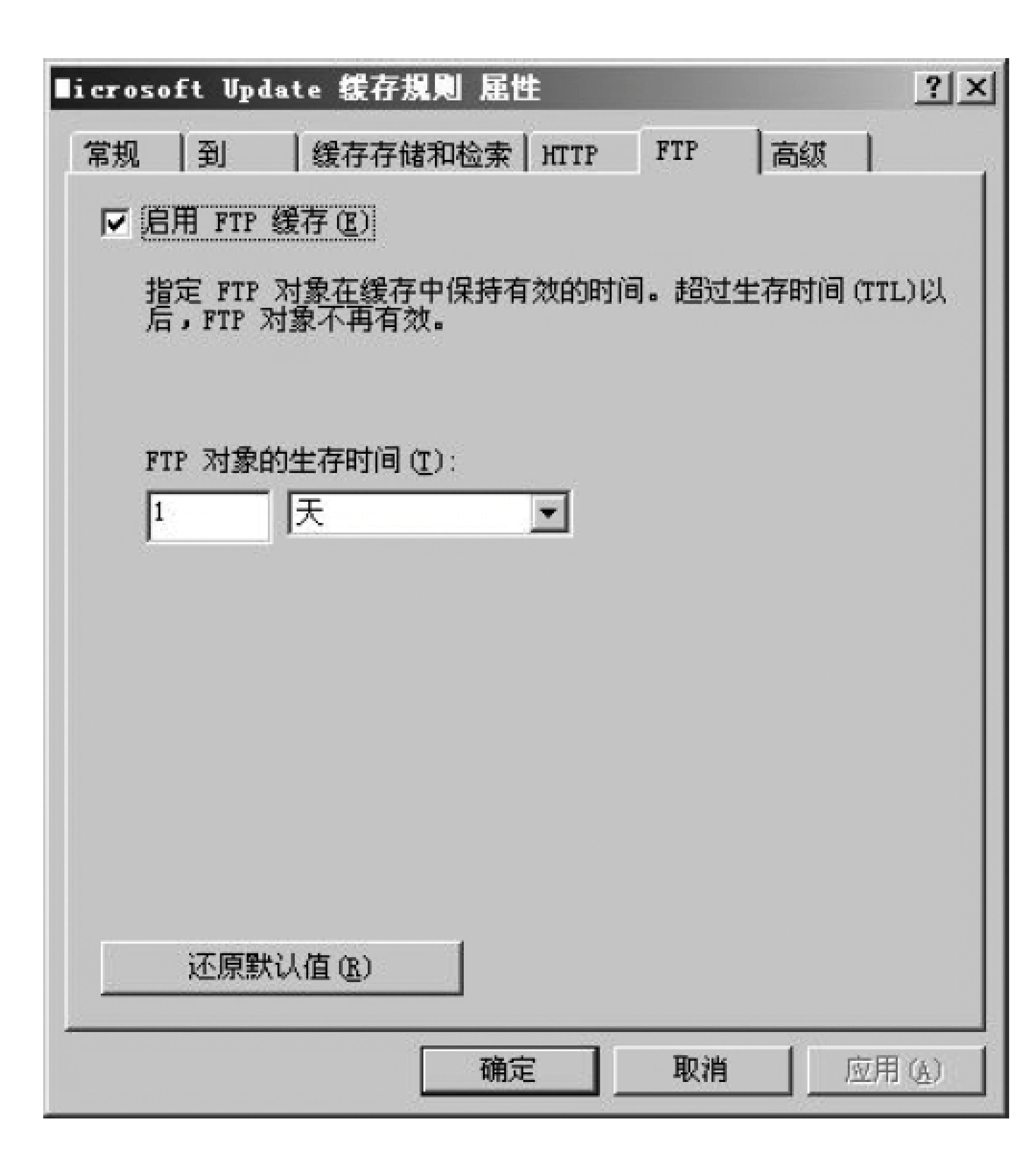
(2) 由系统管理员在 ISA Server 内指定，则设置方法如图 5-67 所示。

- 设置对象的 TTL(内容年龄的百分比)。以图中的 20%为例，若对象从建立(或修改)完成到现在已经过了 10 小时，则该对象在缓存区的有效期限为：10 小时 * 20%=2 小时。
- TTL 时间边界。设置对象有效期限必须介于【不少于】与【不多于】处所指定的时间。
- 对指定过期的源也应用这些 TTL 边界。表示即使网站已经指定对象的有效期限，ISA Server 还会忽视这个期限，并采用设置值来决定对象的有效期限。



如图 5-68 所示，通过 FTP 选项卡来启用或停用 FTP 缓存，设置 FTP 对象在 ISA Server 缓存区的有效期限。

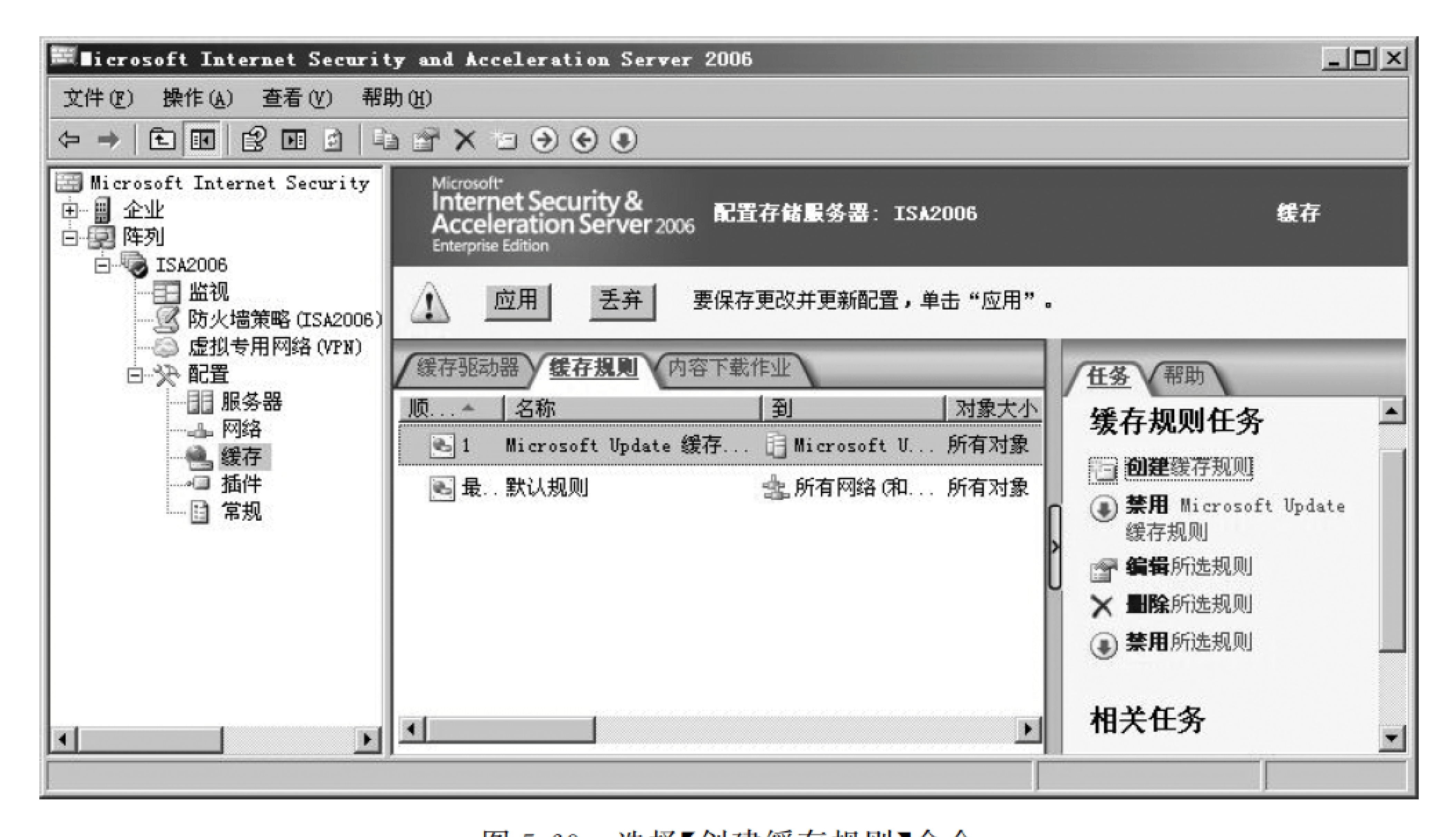

图 5-67 【HTTP】选项卡


图 5-68 【FTP】选项卡

2. 创建缓存规则

系统已经有一个内置的缓存规则，名称为“默认规则”，如果它符合需求，可直接使用此规则。此默认规则的优先级最低，而且不可以被停用。

如果要另外创建新规则，可以在如图 5-69 所示的【缓存规则】选项卡下，单击右边【任务】选项卡中的【创建缓存规则】选项，方法如前面所述。


图 5-69 选择【创建缓存规则】命令



5.6.5 缓存区内容的更新

1. 定时自动下载网页内容

可以排定 ISA Server 在指定时间到达时自动从指定网站下载网页，以便于客户端可以很快地从 ISA Server 缓存区取得所需网页。

定时自动下载网页内容的方法如下：

(1) 如图 5-70 所示，在【ISA 服务器管理】窗口中选择【配置】/【缓存】选项，选择【内容下载作业】选项卡，再单击窗口右边【任务】选项卡的【计划内容下载作业】选项。

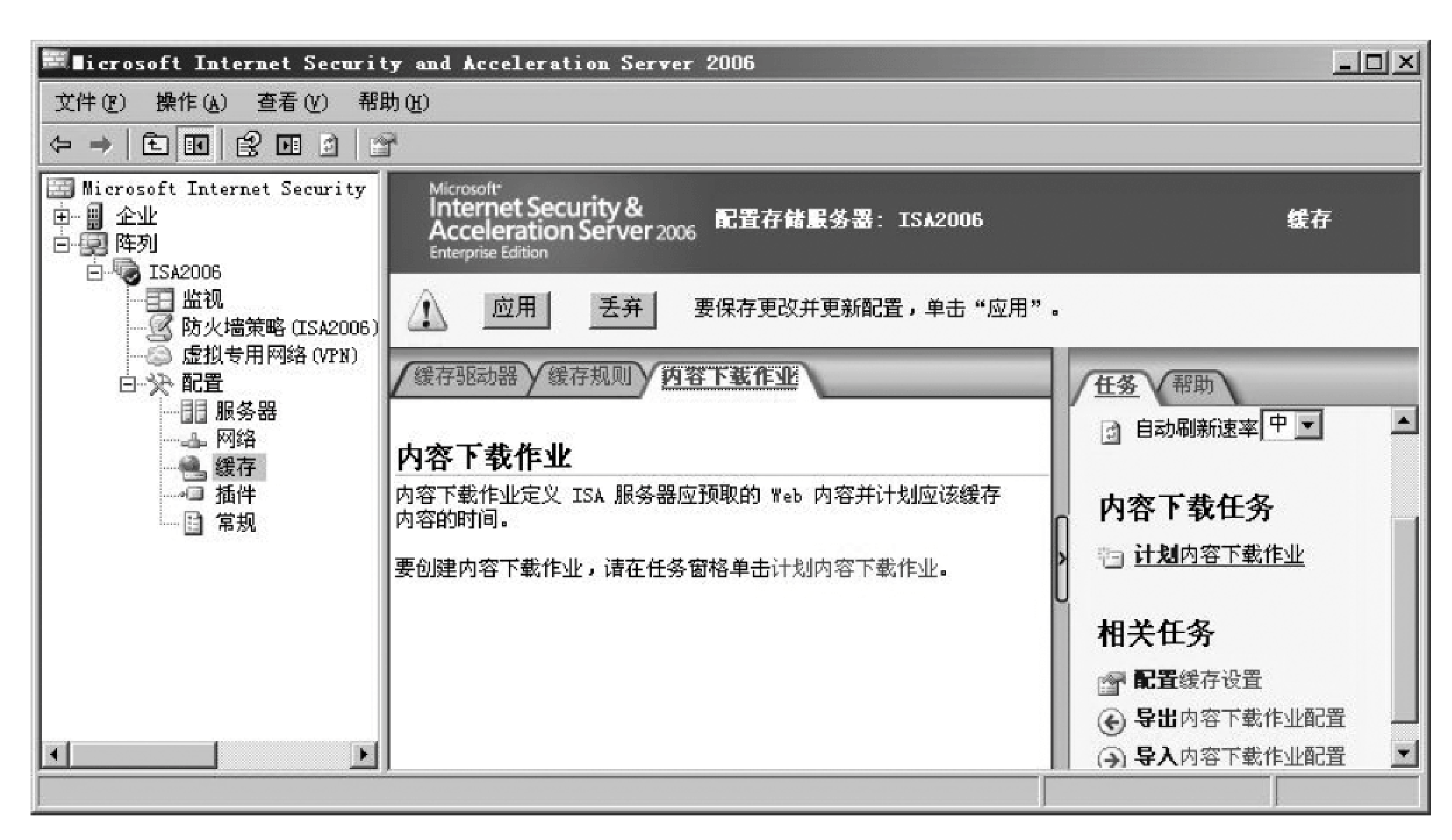


图 5-70 选择【计划内容下载作业】选项

(2) 若是第 1 次单击【计划内容下载作业】选项，则会出现如图 5-71 所示的警告对话框，直接单击【是】按钮。

注意：完成此步骤后，本地主机(指 ISA Server 计算机)就必须以 Web 代理客户端的角色才可以上网。

(3) 如图 5-72 所示，单击【应用】按钮后再单击【确定】按钮。

(4) 与步骤(1)相同，单击图 5-70 右边的【计划内容下载作业】选项。

(5) 在弹出的【欢迎使用内容下载作业向导】对话框中将此计划命名为“新浪新闻”，然后单击【下一步】按钮。

(6) 如图 5-73 所示，选择下载频率(例如“每天”)；在如图 5-74 所示的【每天频率】对话框中设置频率的日期和时间，单击【下一步】按钮。

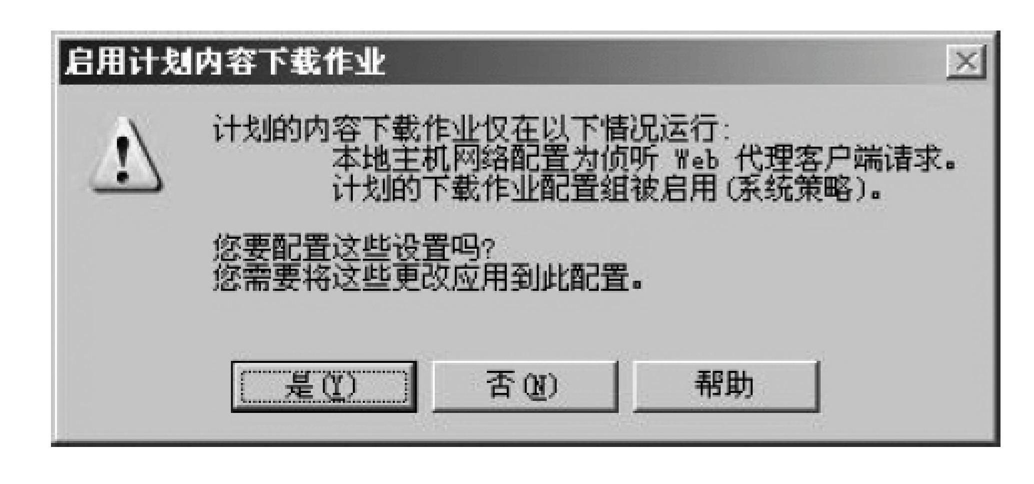


图 5-71 【启用计划内容下载作业】警告对话框





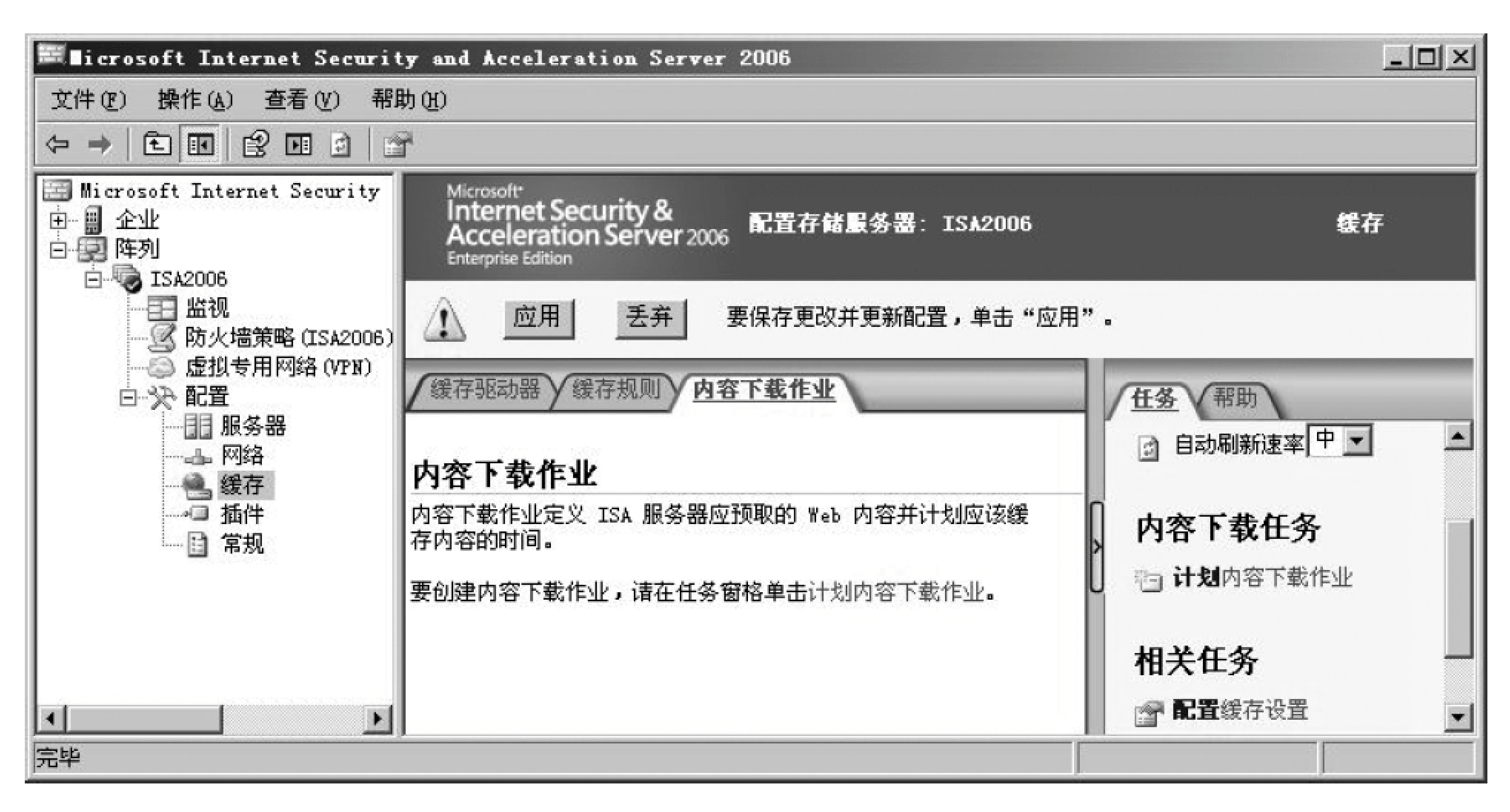


图 5-72　单击【应用】按钮

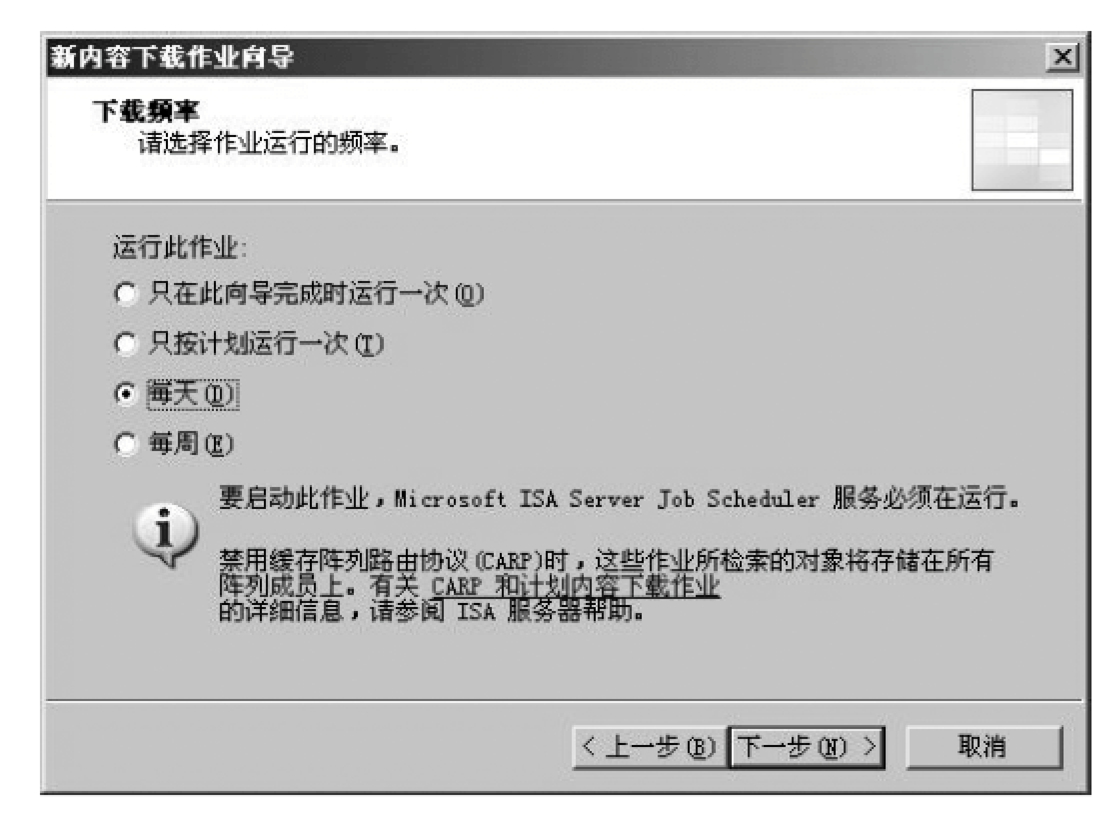


图 5-73　【下载频率】对话框

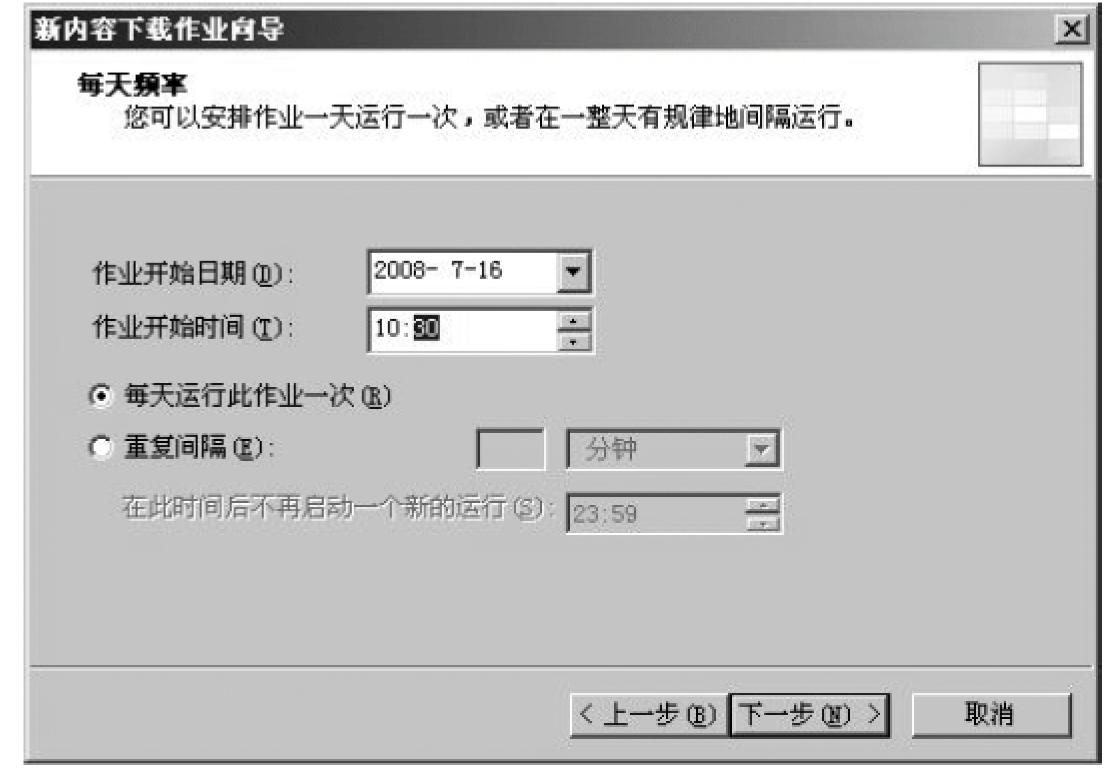


图 5-74　【每天频率】对话框

(7) 如图 5-75 所示,在【内容下载】对话框中设置要从哪一个网站下载网页,并设置【作业限制】选项区的选项,单击【下一步】按钮。

(8) 如图 5-76 所示,在【内容缓存】对话框中设置缓存内容与设置内容的生存周期(TTL),然后单击【下一步】按钮。

(9) 最后在【正在完成计划内容下载作业向导】对话框中,单击【完成】按钮。

2. 删除缓存区的数据

由于 ISA Server 缓存区中的数据有一个有效期限(如 2 小时),虽然网站的内容已经更新,但是缓存区中内容还是旧的,如何迅速更新缓存区中的内容呢?此时最快的解决方法就是手动将 ISA Server 缓存区的数据删除。删除缓存区数据的步骤如下:

(1) 停止防火墙服务。如图 5-77 所示,在【ISA 服务器管理】窗口中选择【监视】/【服务】选项,再选择 Microsoft Firewall,然后单击窗口右边【任务】选项卡中的【停止选择的服务】选项。

(2) 删除缓存文件。如图 5-78 所示,删除文件夹 urlcache 内的 Dir1. cdat 文件(假设缓存硬盘驱动器在 C 盘)。





图 5-75 【内容下载】对话框

新内容下载作业向导

内容缓存

请指定要缓存的内容和在过期前对象在缓存中生存的时间。

缓存内容

缓存所有内容(L)

如果源和请求的头表明要缓存，或者内容是动态的，内容将被缓存(S)

如果源和请求的头表明要到缓存，内容将被缓存(U)

生存周期(TTL)

根据缓存规则将内容过期(R)

设置 TTL，如果它没有在响应中定义(T)

替代对象的 TTL(O)

用新的 TTL(分钟)标记下载的对象(D): 60

生存周期是内容在过期前在缓存中保存的时间。

< 上一步(B) 下一步(N) > 取消

图 5-76 【内容缓存】对话框

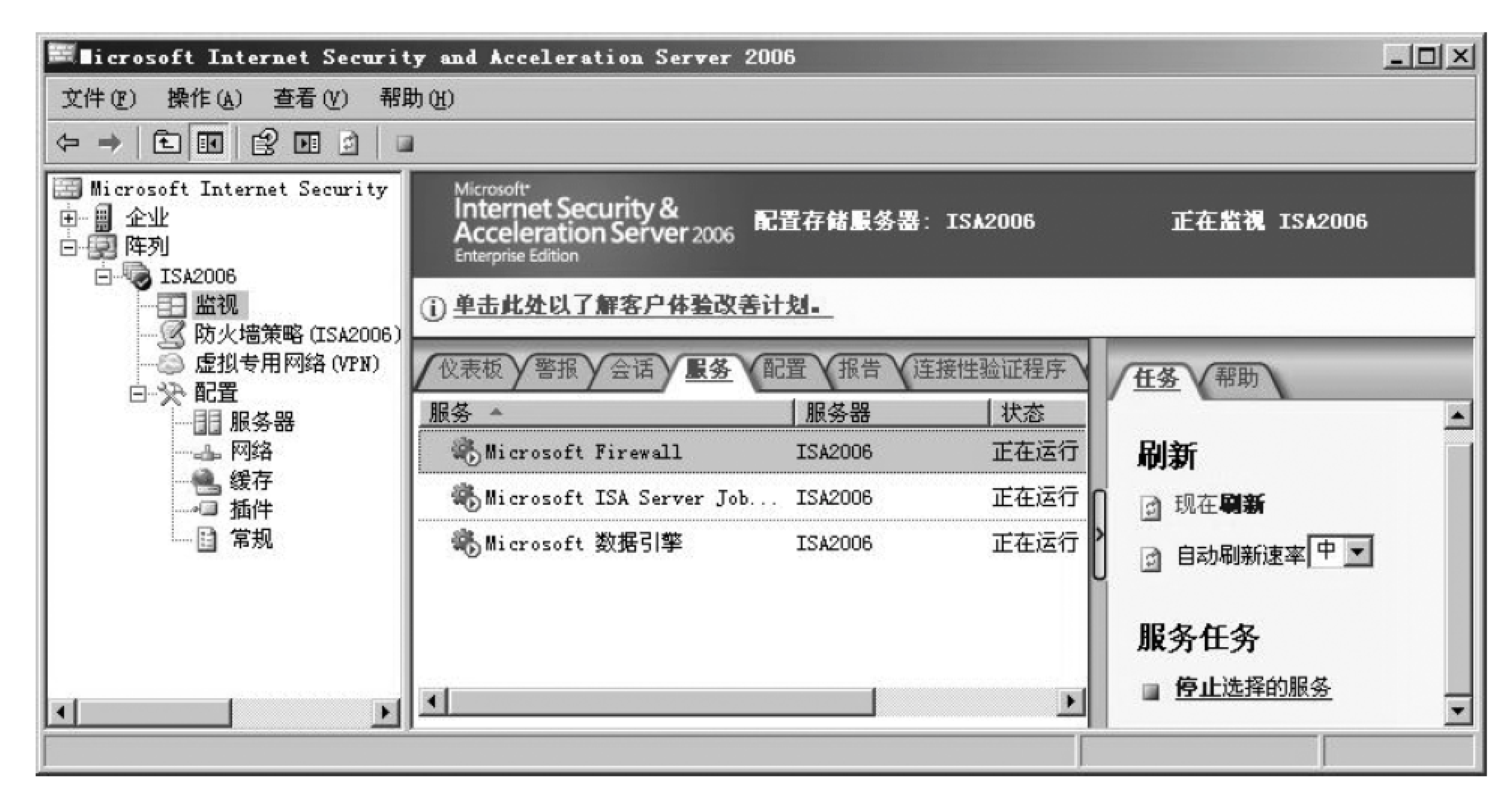


图 5-77 选择【停止选择的服务】命令



图 5-78 删除缓存文件



(3) 重新启动防火墙服务。如图 5-79 所示,在【ISA 服务器管理】窗口单击右边【任务】选项卡中的【启动选择的服务】选项。



图 5-79　单击【启动选择的服务】选项

5.7　ISA Server 客户端的应用

5.7.1　ISA Server 客户端概述

ISA Server 支持三种不同的客户端,它们分别有着不同的配置,支持的网络协议也有所不同,与 ISA Server 之间的沟通方式也略微有些不同。

- Web 代理客户端(Web Proxy client):Web 代理客户端只能利用网页应用程序(例如浏览器)访问 Internet 的 HTTP、HTTPS 与 FTP 对象。Web 代理客户端是将请求传递给 ISA Server 的连接端口 8080,而当 ISA Server 接收到 Web 代理客户端的请求后,会将此请求委托防火墙服务来决定是否允许。ISA Server 防火墙会从缓冲区来读取 Web 代理客户端所请求的对象,而且也会将从 Internet 取得的对象保存到缓冲区。
- SecureNAT 客户端(SecureNAT client):SecureNAT 客户端能够通过 ISA Server 来访问 Internet 的 TCP、UDP、HTTP、HTTPS、FTP 与其他网络协议的资源。SecureNAT 客户端是利用默认网关将请求传递给 ISA Server,而当 ISA Server 接收到 SecureNAT 客户端的请求后,会先利用 NAT driver(Network Address Translation driver)将数据包的源地址转换为一个对外有效的 IP 地址,然后再将此请求转交给防火墙服务,并搭配适当的筛选器,来决定是否允许此请求。
- 防火墙客户端(Firewall client):这些客户端必须另外安装 Microsoft Firewall Client。防火墙客户端是将 HTTP 请求传递给 ISA Server 的连接端口 8080,将非 HTTP 请求传递给 ISA Server 的连接端口 1745,而当 ISA Server 接收到防火墙客



户端的请求后，会将此请求转交给防火墙服务，并搭配适当的筛选器，来决定是否允许此请求。

表 5-1 列出各个客户端的基本差异。

表 5-1 各个客户端的基本差异

特　点	Web 代理客户端	SecureNAT 客户端	防火墙客户端
支持的操作系统	所有的操作系统	所有的操作系统	只支持 Windows 操作系统
支持的网络协议	HTTP、HTTPS、FTP		
是否需要额外安装软件	否，但是需要浏览器配置	否，但是需要网络配置	是
HTTP 验证用户身份	是	只有 VPN 客户端	是
非 HTTP 验证用户身份	不支持访问	只有 VPN 客户端	是
选择适当的客户端	不建议选用	发布网站或服务器	普通用户

5.7.2 搭建 ISA Server 客户端测试环境

如图 5-80 所示，搭建 ISA Server 客户端测试环境。

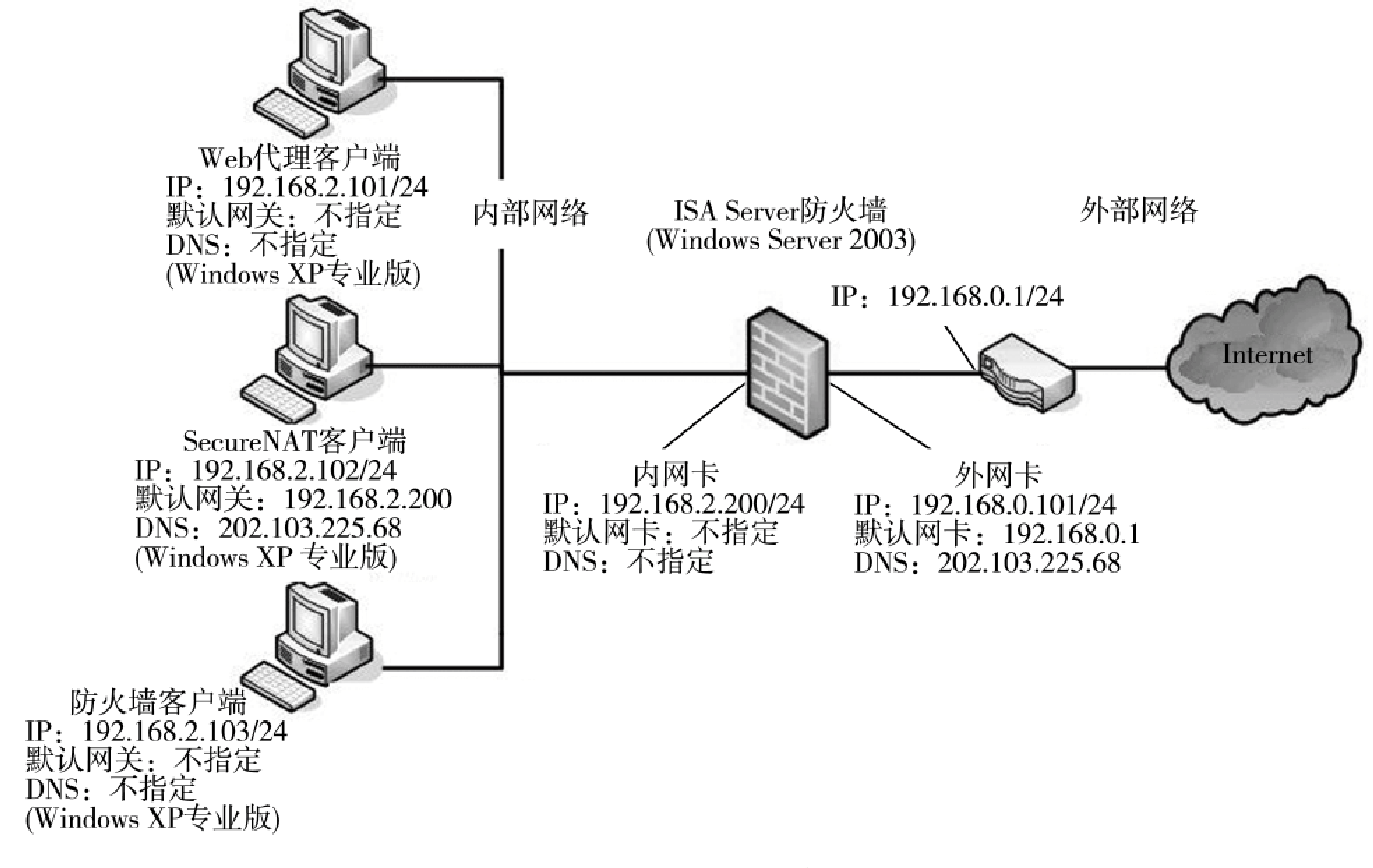


图 5-80 ISA Server 客户端测试环境

5.7.3 ISA Server 的配置

下面介绍如何在 ISA Server 中创建规则，开放内部网络用户可以访问外部网站。



1. 防火墙规则的开放

修改原来创建的一个名为“允许本地主机访问外部网站”的访问规则(此规则开放让ISA Server这台本地主机可以访问Internet的网页),让内部网络的客户端也可以访问Internet的网页对象。方法如下:

(1) 在【ISA服务管理】窗口左侧列表中选择【防火墙策略】选项,然后双击【允许本地主机访问外部网站】访问规则,如图5-81所示。

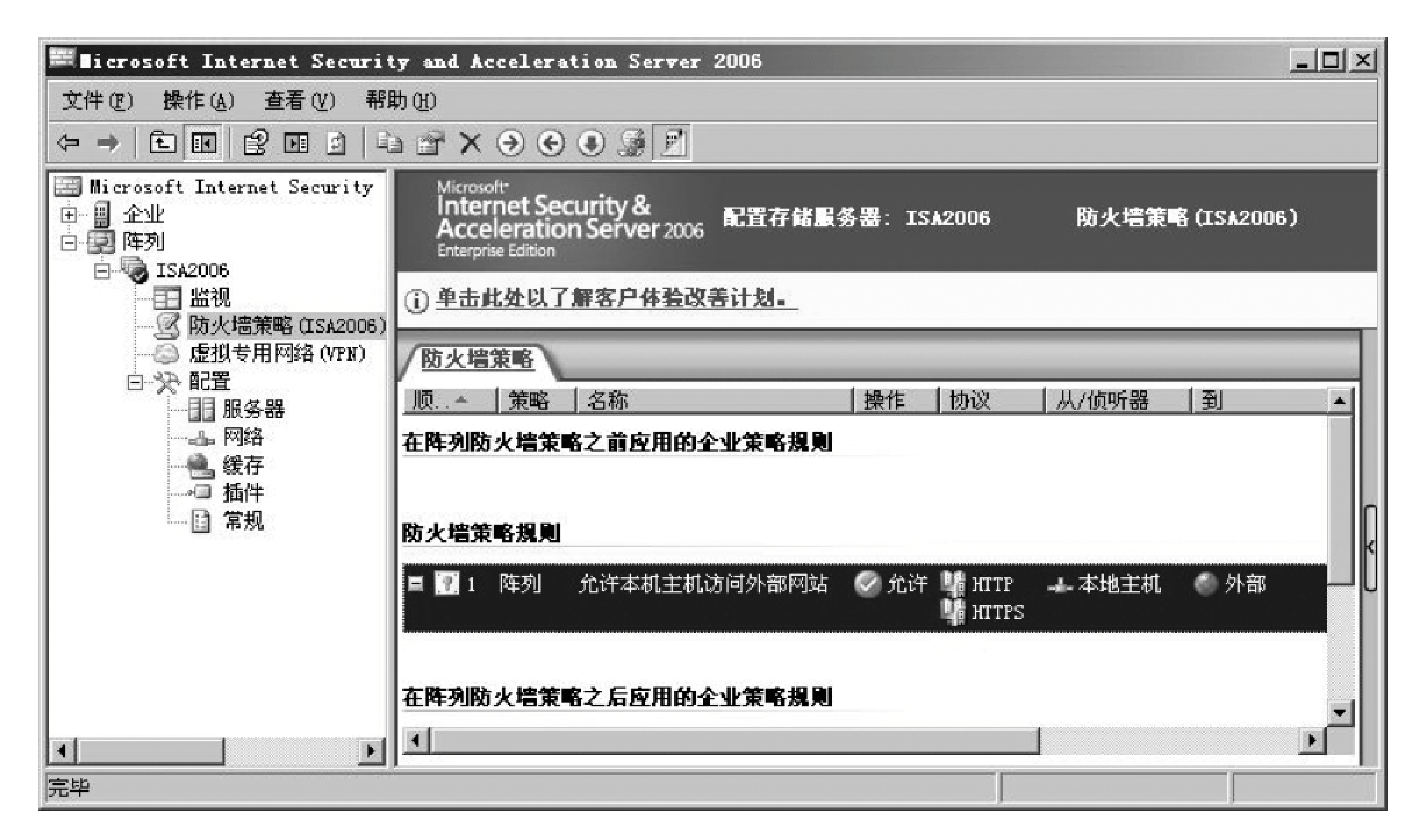


图5-81　双击【允许本地主机访问外部网站】访问规则

(2) 将访问规则名称改为“允许内部和本地主机访问外部网站”,如图5-82所示。

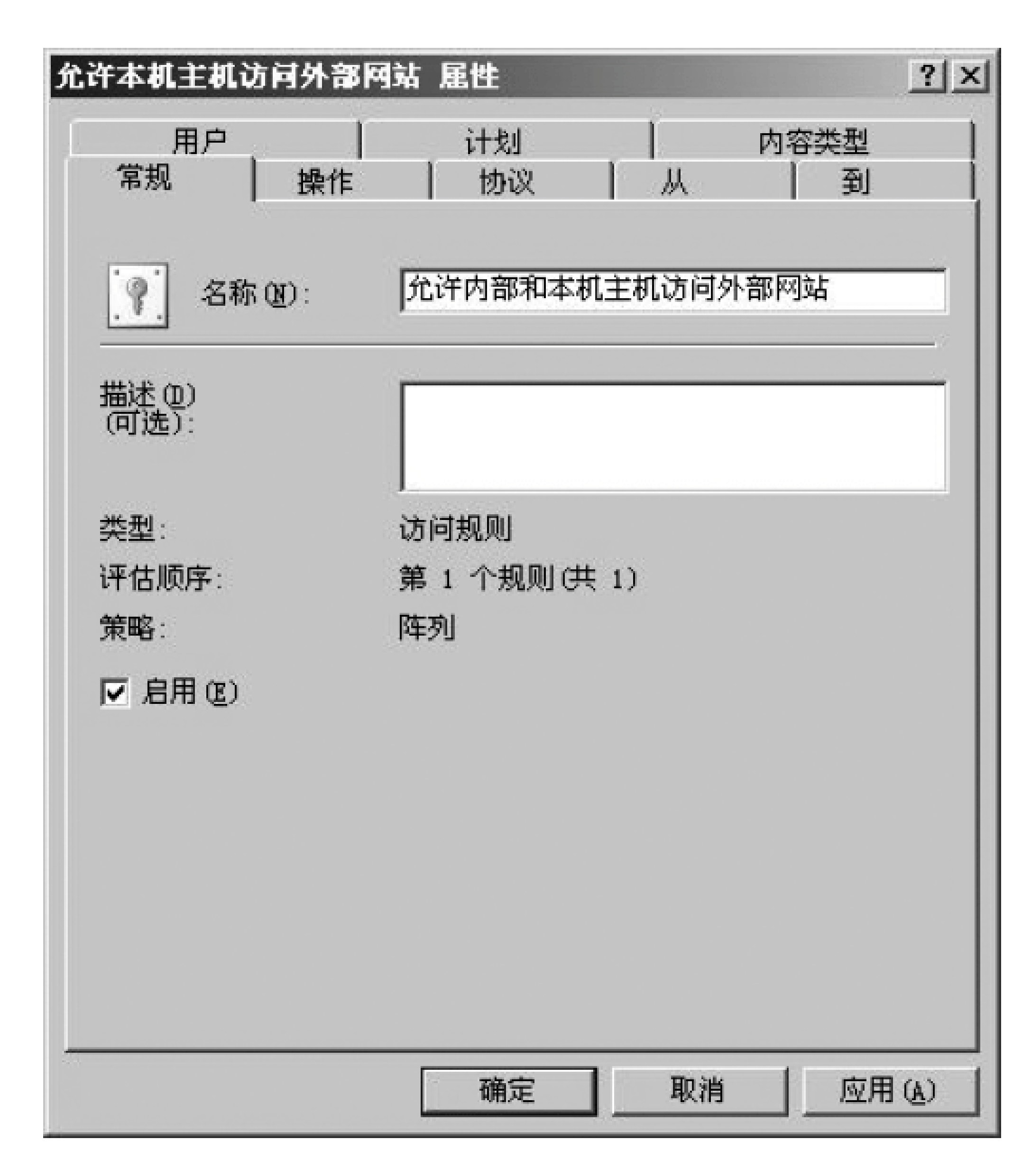


图5-82　更改访问规则名称



（3）选择【从】选项卡，单击【添加】按钮，选择网络之下的【内部】选项，依次单击【添加】按钮、【关闭】按钮、【确定】按钮，如图 5-83 所示。



图 5-83　将【内部】网络添加到【从】选项卡

（4）依次单击【应用】按钮和【确定】按钮，如图 5-84 所示。

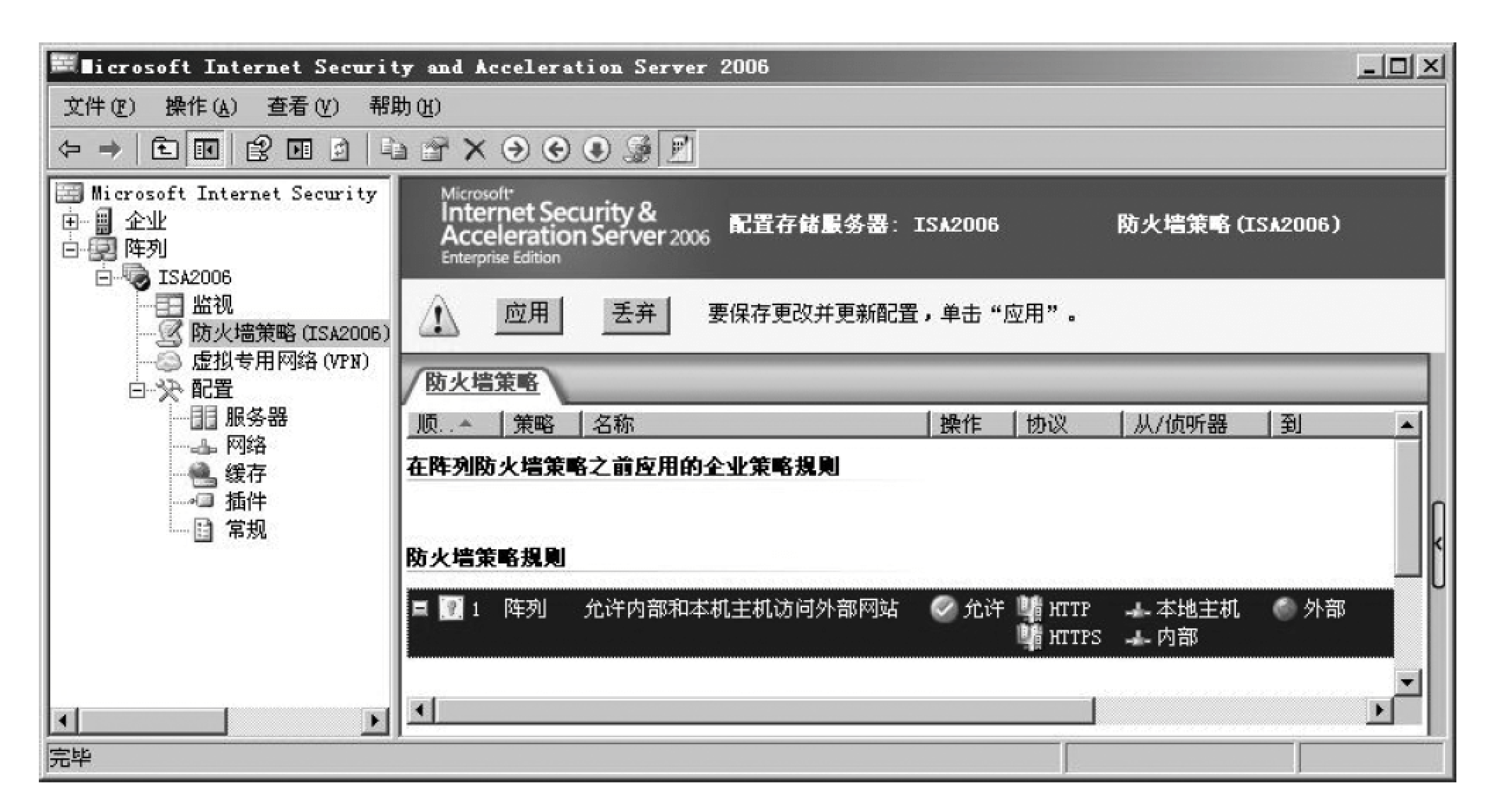


图 5-84　单击【应用】按钮

2．确认可接收“Web 代理客户端”的请求

（1）在【ISA 服务管理】窗口中选择【配置】选项下的【网络】选项，再双击【网络】选项卡中的【内部】选项，如图 5-85 所示。





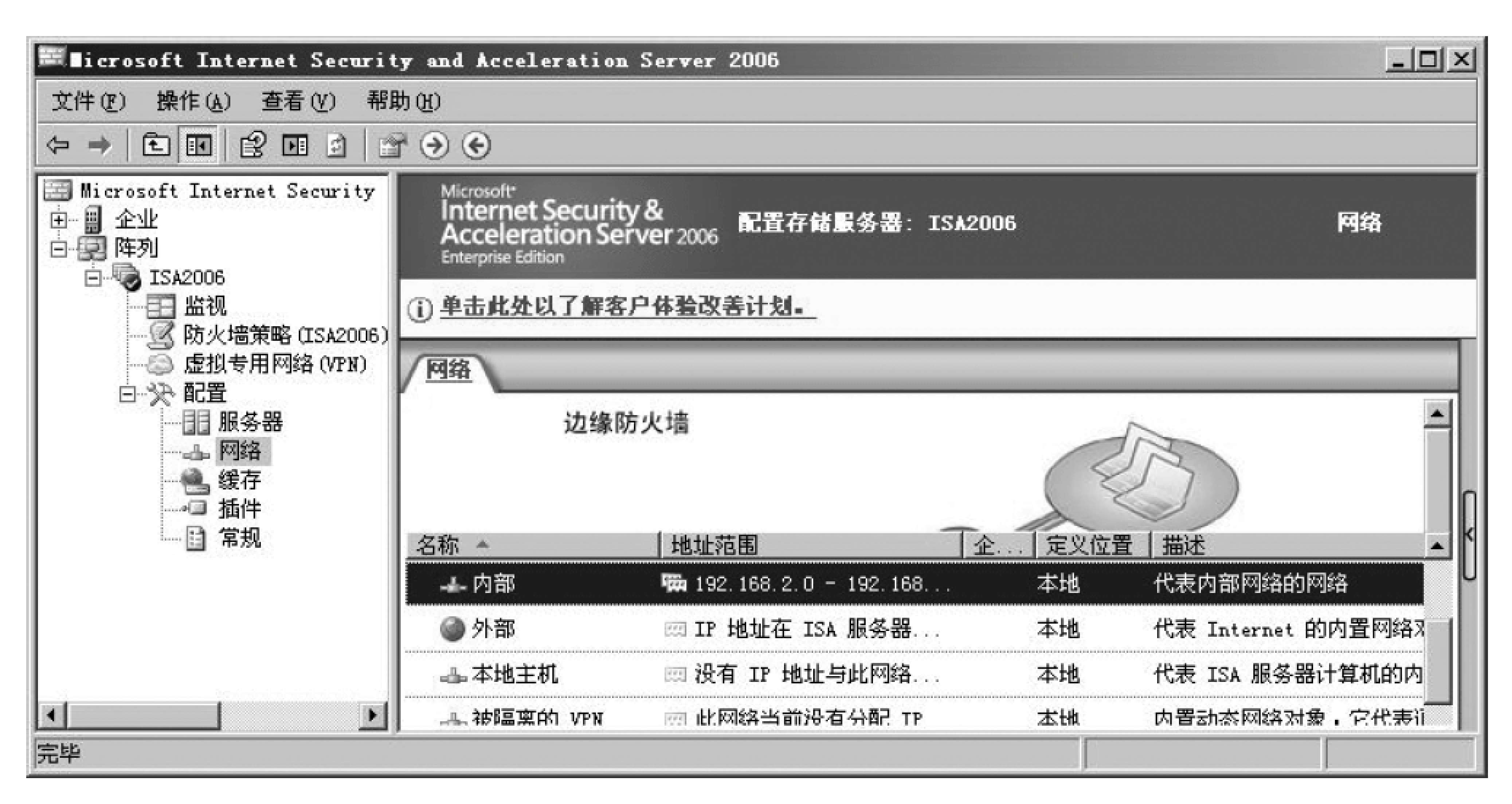


图 5-85　双击【内部】网络

（2）在【内部 属性】对话框中，选择【Web 代理】选项卡，选中【为此网络启用 Web 代理客户端连接】(注意：Web 代理服务的连接端口为 8080)，如图 5-86 所示。

（3）单击【确定】按钮。

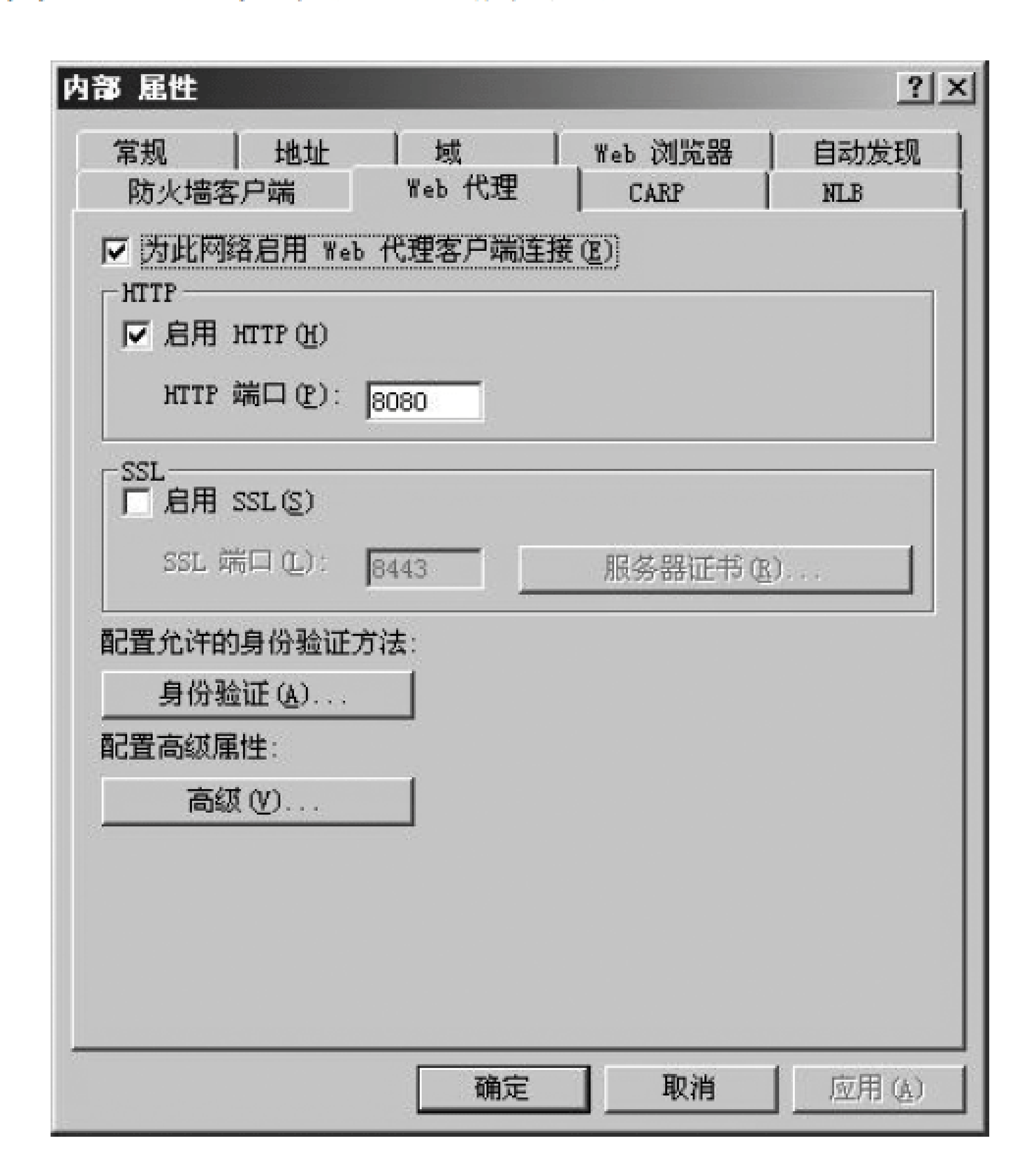


图 5-86　【Web 代理】选项卡

5.7.4　Web 代理客户端的配置

所有的操作系统都可以扮演 Web 代理客户端的角色，不过只支持 HTTP、HTTPS 与 FTP 网络协议。

ISA Server 默认通过连接端口 8080 来侦听 Web 代理客户端的请求。当 ISA Server 收到 Web 代理客户端访问 Internet 网页或 FTP 对象的请求时，会由防火墙服务来决定是否允许此请求，如果允许，接下来会通过网页代理筛选器来检查缓冲区是否有客户端所需的对象，如果有，防火墙服务会将对象传递给客户端；如果没有，则上网下载对象，并通过网页代理筛选器将下载的对象保存到缓冲区。

需要在 Web 代理客户端的应用程序内指定将 ISA Server 当作是代理服务器，该应用程序才会将访问 Internet 网页与 FTP 对象的请求，传递给 ISA Server 的连接端口 8080。其配置步骤如下：

（1）运行 IE(Internet Explorer)浏览器，如图 5-87 所示，再选择【工具】/【Internet 选项】命令。

（2）选择【连接】选项卡，单击【局域网设置】按钮，如图 5-88 所示。





图 5-87 Internet 选项

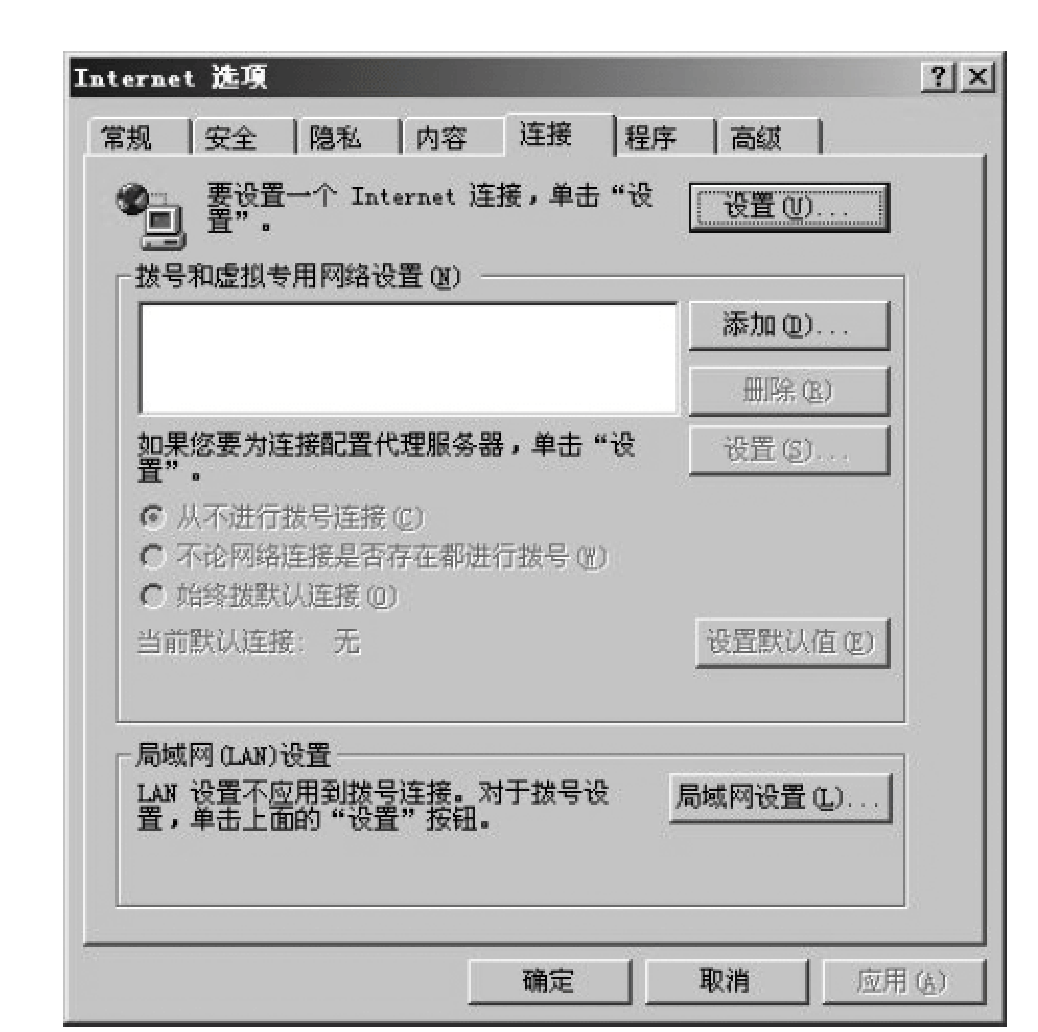


图 5-88 【连接】选项卡

(3) 在【局域网(LAN)设置】对话框中,选中【为 LAN 使用代理服务器】选项,将 ISA Server 内网卡的 IP 地址 192.168.2.200 输入到【地址】文本框中,将连接端口 8080 输入到【端口】文本框中,如图 5-89 所示。

完成 5.7.3 小节 ISA Server 的配置和本节 Web 代理客户端的配置后,就可以在此 Web 代理客户端利用 IE 浏览器上网测试,此时可以通过 ISA Server 下载所需网页,这些下载的对象也会被保存到 ISA Server 缓冲区。

5.7.5 SecureNAT 客户端的配置

所有的操作系统都可以扮演 SecureNAT 客户端的角色,并支持 TCP、UDP、HTTP、HTTPS、FTP 与其他网络协议。如果要将内部或 DMZ 网络内的服务器(例如电子邮件服务器、网站等),发布给 Internet 用户访问,最好将这台服务器配置为 SecureNAT 客户端。

1. SecureNAT 客户端的配置

将 SecureNAT 客户端的默认网关指定为 ISA Server 内网卡的 IP 地址,再将 SecureNAT 客户端的首选 DNS 服务器指定到公司内部的 DNS 服务器或 Internet 上任何一台可以正常运作的 DNS 服务器,如图 5-90 所示。

2. 开放 DNS 流量

SecureNAT 客户端在解析 DNS 主机名时,如果需要通过 ISA Server 来向外部查询,就在 ISA Server 开放让从内部网络来的 DNS 流量能够通过。开放 DNS 流量的步骤如下:

(1) 在【ISA 服务管理】窗口中从左侧列表中选择【防火墙策略】选项,单击窗口右边【任务】选项卡中的【创建访问规则】选项,如图 5-91 所示。







图 5-89　【代理服务器】设置

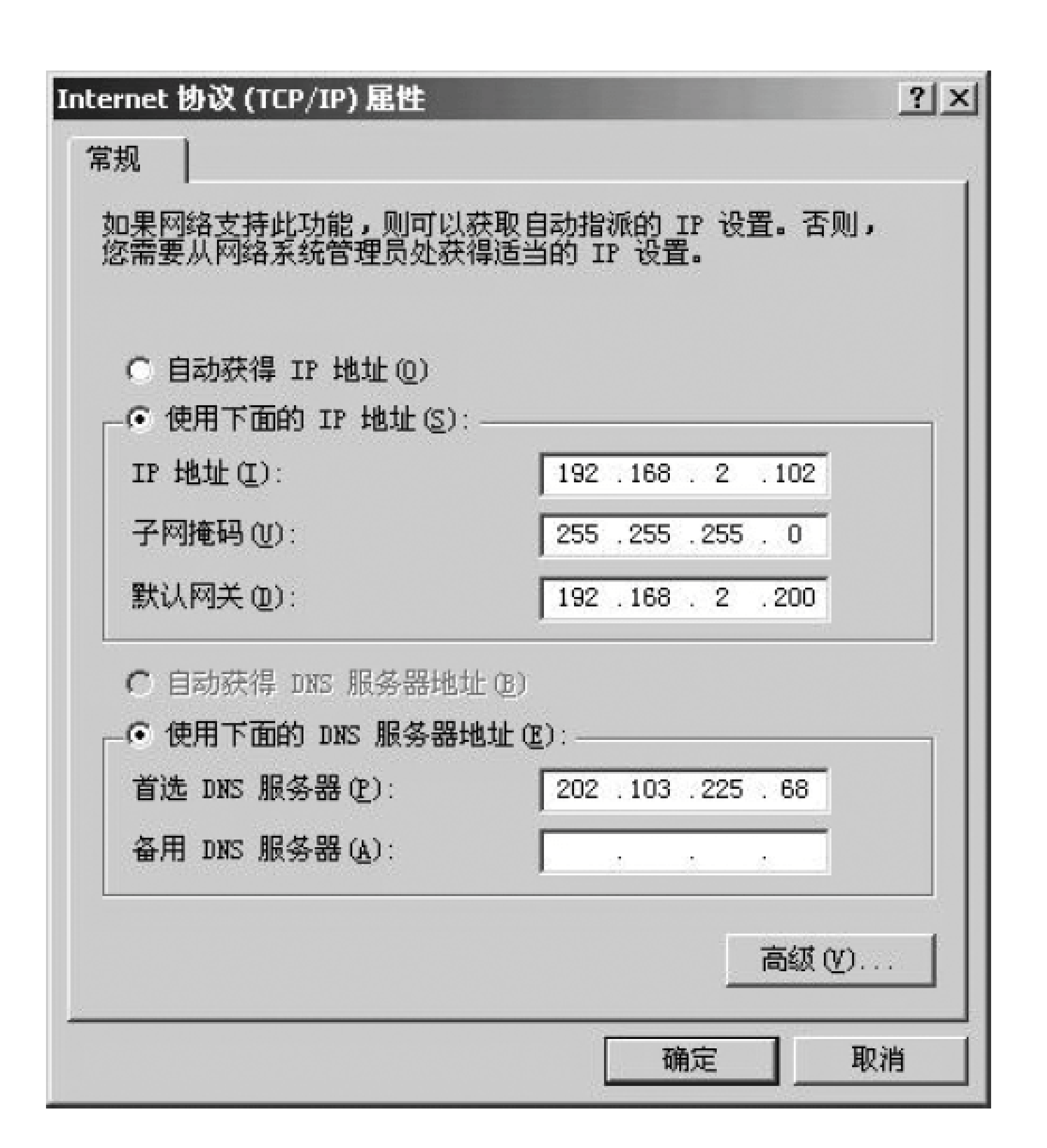


图 5-90　SecureNAT 客户端 IP 参数



图 5-91　单击【创建访问规则】选项

（2）在【欢迎使用新建访问规则向导】对话框中为此访问规则命名（例如“允许 DNS 请求”）。

（3）在【新建访问规则向导】对话框中选择【允许】选项，单击【下一步】按钮，从【此规则应用到】下拉列表中选择“所选的协议”，单击【添加】按钮，如图 5-92 所示。

（4）在【添加协议】对话框中选择“DNS”通用协议，依次单击【添加】按钮、【关闭】按钮、【下一步】按钮，如图 5-93 所示。

（5）在新建访问规则向导的【访问规则源】对话框中，选择此规则的“访问规则源”。要让内部网络所有计算机的 DNS 请求通过 ISA Server 防火墙，因此选择“内部 ”选项，如图 5-94 所示。





图 5-92 【协议】对话框



图 5-93 选择【DNS】通用协议

(6) 在新建访问规则向导的【访问规则目标】对话框中,选择此规则的“访问规则目标”。要允许向外部所有的 DNS 服务器查询,选择“外部”选项,如图 5-95 所示。

(7) 在【用户集】对话框中单击【下一步】按钮,将此规则应用到所有用户。

(8) 在【完成新建访问规则向导】对话框中,单击【完成】按钮。

(9) 在【ISA 服务器管理】窗口中依次单击【应用】按钮、【确定】按钮。

完成以上配置后,利用这台 SecureNAT 客户端计算机上网测试,此时可以通过 ISA Server 访问所需的网页。





图 5-94　添加【内部】网络到【访问规则源】



图 5-95　添加【外部】网络到【访问规则目标】



5.7.6 防火墙客户端的配置

要配置为防火墙客户端，客户端必须是 Windows 平台，而且还要安装 Microsoft Firewall Client 软件。

1. 客户端的配置

防火墙客户端的 TCP/IP 只需要配置 IP 地址和子网掩码即可，如图 5-96 所示。

图 5-96 防火墙客户端的 IP 参数

2. 安装 Microsoft Firewall Client 软件

客户端安装了 Microsoft Firewall Client 软件后，当客户端的 Winsock 应用程序请求与其他网络的计算机沟通时，会由 Microsoft Firewall Client 负责将此请求传递给 ISA Server。但是如果要沟通的对象是内部网络的其他计算机，则此沟通请求并不会传递给 ISA Server。安装方法如下：

（1）在 ISA Server 中创建规则，开放 NetBIOS 会话、NetBIOS 名称服务、NetBIOS 数据报三个网络协议，方向为从“内部网络”到“本地主机”，以便防火墙客户端解析 ISA Server 的计算机名，如图 5-97 所示。



图 5-97 创建访问规则

（2）确认 ISA Server 是否可以接收内部网络防火墙客户端访问 Internet 的请求。如图 5-98 所示，双击【网络】选项卡的【内部】选项，在【内部属性】对话框中选择【防火墙客户端】选项卡，选中【启用此网络的防火墙客户端支持】选项，在【ISA 服务器名称或 IP 地址】文



本框输入 ISA Server 内网卡的 IP 地址(例如 192.168.2.200),单击【确定】按钮。

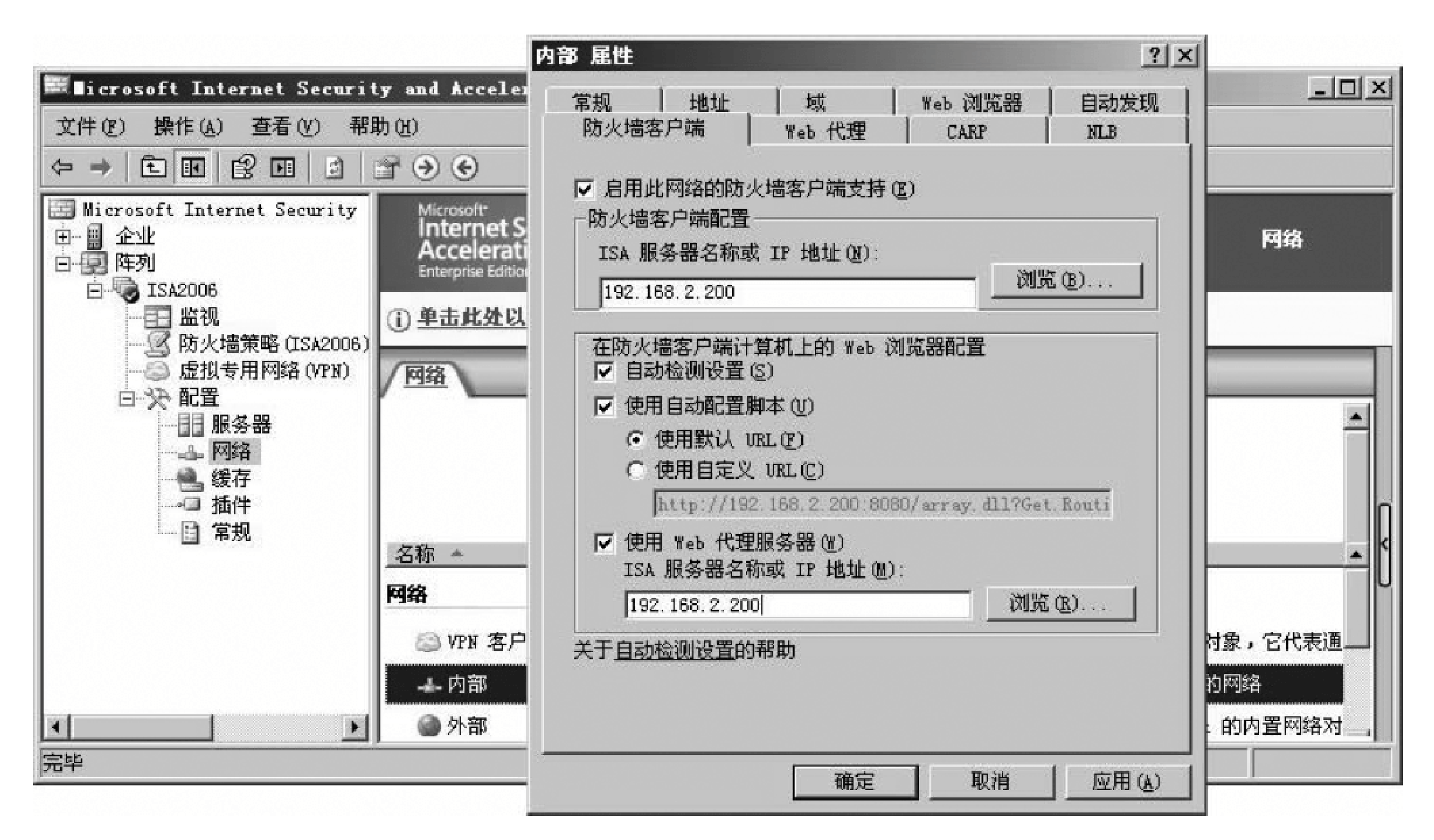


图 5-98 【内部】网络的【防火墙客户端】选项卡

(3) Microsoft Firewall Client 软件是放在 ISA Server 软件包的 client 文件夹内,执行此文件夹中的 setup.exe 程序,安装界面如图 5-99 所示,选择【连接到此 ISA 服务器计算机】单选按钮,然后输入 ISA Server 的 IP 地址或主机名(例如输入 ISA Server 内部网卡的 IP 地址 192.168.2.200)。

3. "防火墙客户端"默认也是"Web 代理客户端"

当防火墙客户端安装了 Microsoft Firewall Client 后,系统自动会在 Internet Explorer 浏览器内将 ISA Server 配置为代理服务器,客户端利用 Internet Explorer 访问 Internet 的网页与 FTP 对象时,该防火墙客户端被视为 Web 代理客户端,如图 5-100 所示。

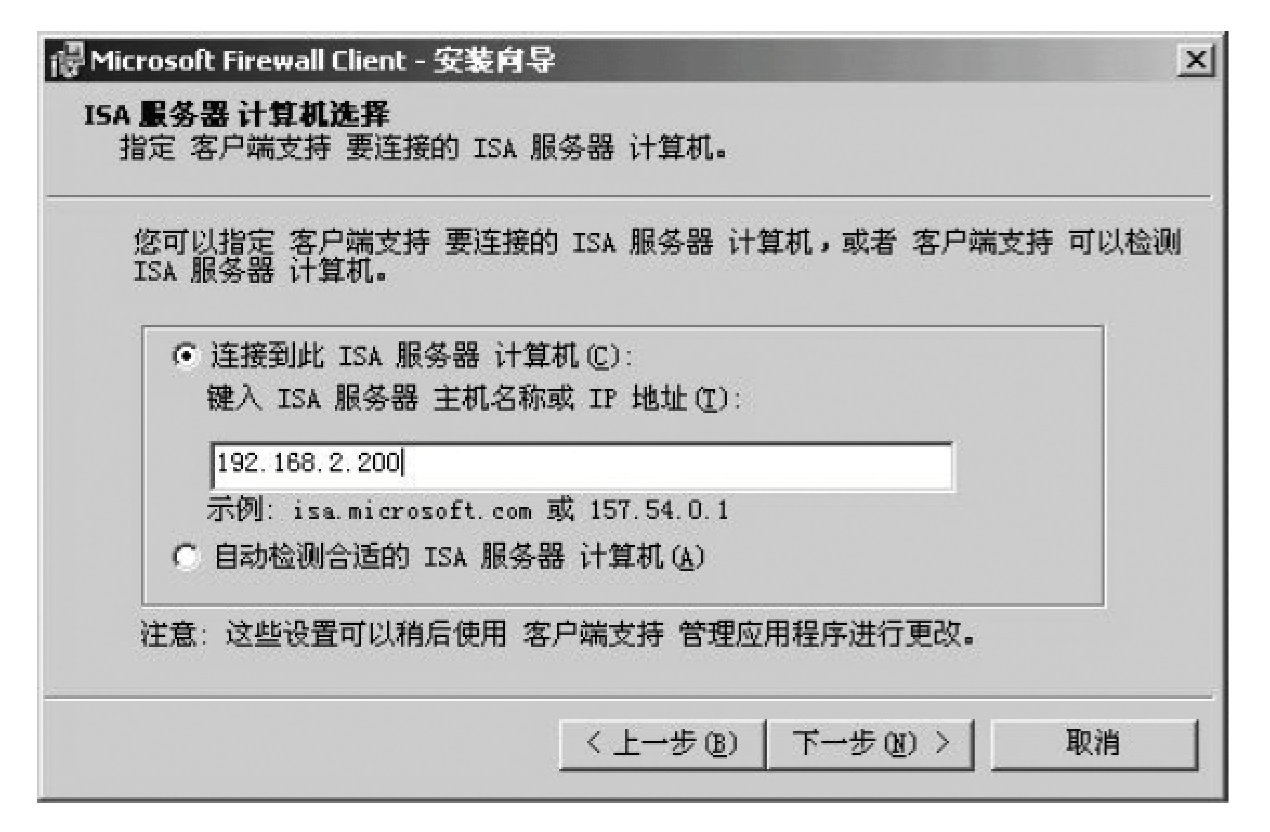


图 5-99 【ISA 服务器计算机选择】对话框

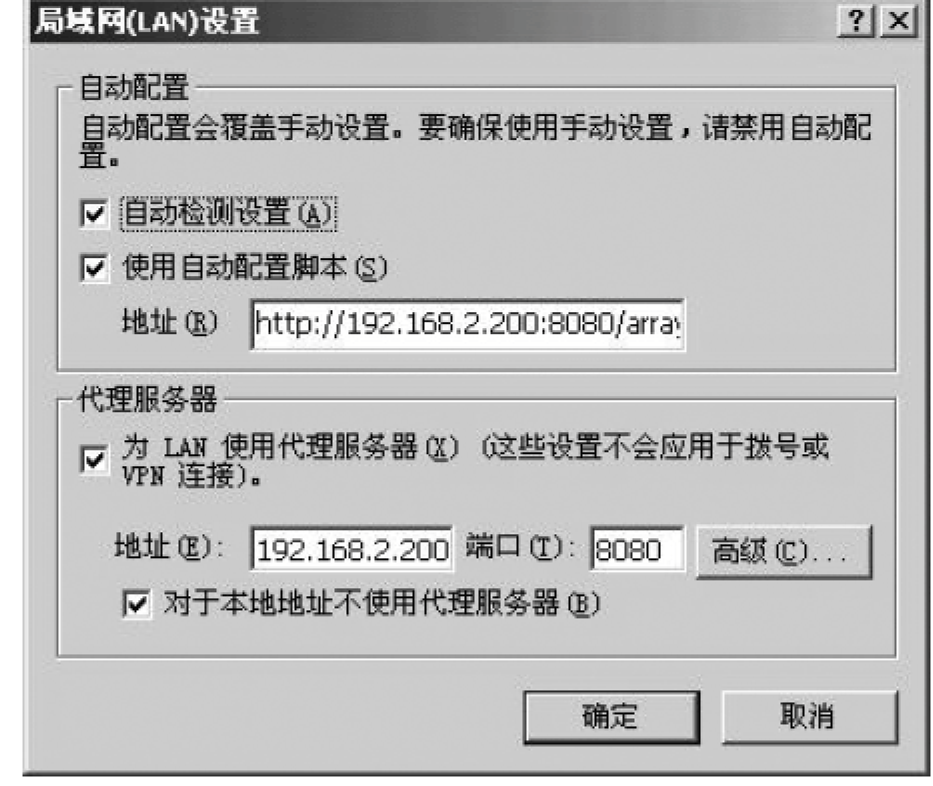


图 5-100 【局域网(LAN)设置】对话框



5.8 开放访问 Internet

5.8.1 访问 Internet 概述

一般用户上网的目的，主要就是访问网页、访问 FTP 文件、收发电子邮件等，本实验介绍如何在 ISA Server 开放这些流量。

在 ISA 中要开放这些规则，需要创建如下 4 个访问规则。

- 允许内部到本地主机的 NetBIOS 请求，让内部客户端可以解析 ISA Server 主机的 NetBIOS 计算机名称。
- 允许内部到外部的 DNS 请求，让内部所有客户端可以向外部 DNS 服务器查询。
- 允许内部与本地主机访问外部网站与 FTP，让内部客户端与本地主机可以连接位于 Internet 的网站与 FTP 服务器(假设网站连接端口为 80，SSL 网站为 443，FTP 为 21)。
- 允许内部到外部的 SMTP 与 POP3 请求，让内部客户端可以接收外部 POP3 服务器内的邮件，也让用户可以通过外部 SMTP 服务器来收发电子邮件。

5.8.2 创建访问规则

如图 5-101 所示，在【ISA 服务器管理】窗口左侧列表中单击【防火墙策略】选项，单击窗口右边【任务】选项卡中的【创建访问规则】选项，规则的创建的方法和步骤如 5.4.3 小节所述。可以创建如图 5-102 所示的 4 个访问规则。

- 允许内部到本地主机的 NetBIOS 请求。
- 允许内部到外部的 DNS 请求。
- 允许内部和本地主机访问外部网站与 FTP。
- 允许内部到外部的 SMTP 与 POP3 请求。

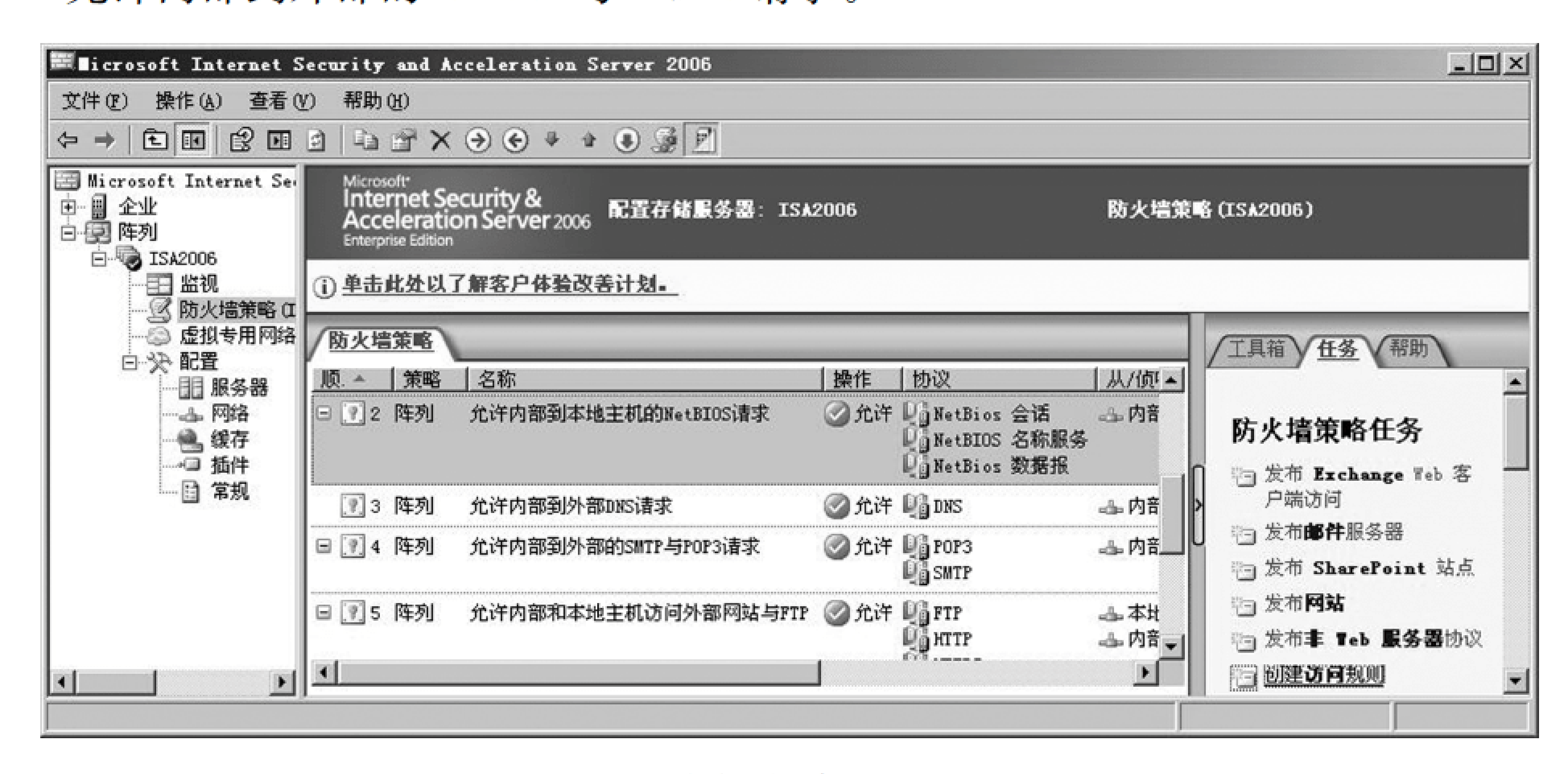


图 5-101 单击【创建访问规则】选项





图 5-102　创建了 4 个访问规则

5.8.3　开放 FTP 写入的功能和开放非标准连接端口

1. 开放 FTP 写入的功能

由于 ISA Server 默认开放给用户对 FTP 服务器的权限是“只读”，因此，即使 FTP 服务器本身已经开放“写入”权限，用户通过 ISA Server 仍然无法上传或修改文件。在 ISA Server 内开放 FTP 写入权限的步骤如下。

(1) 在如图 5-102 所示的【ISA 服务器管理】窗口中，双击【允许内部和本地主机访问外部网站与 FTP】。

(2) 在打开的【允许内部和本地主机访问外部网站与 FTP 属性】对话框中选择【协议】选项卡，单击【筛选】按钮并选择【配置 FTP】命令，如图 5-103 所示；在打开的【配置 FTP 协议策略】对话框中，取消选中【只读】复选框，如图 5-104 所示。

(3) 回到【ISA 服务器管理】窗口，依次单击【应用】按钮、【确定】按钮。

2. 开放非标准连接端口

前面针对网页、FTP 与电子邮件所开放的规则，都是假设它们所使用的 TCP 连接端口是标准的(例如网站为 80、FTP 为 21、SMTP 为 25、POP3 为 110)。如果某个服务器软件拥有自己的连接端口，或者网站等服务器使用不标准连接端口，就需要先另外创建新的协议，然后在访问规则内开放这个新的协议。

假设要开放内部网络的用户可以访问连接端口被设置为 9988 的网站，则要先创建一个连接端口为 9988 的新协议。操作步骤如下：

(1) 在【ISA 服务器管理】窗口中，在左侧列表中选择【防火墙策略】选项，再单击窗口右边的【工具箱】选项卡，选择【协议】/【新建】/【协议】命令，如图 5-105 所示。

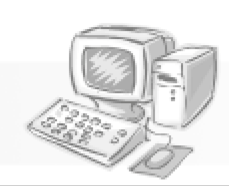





图 5-103 【协议】选项卡

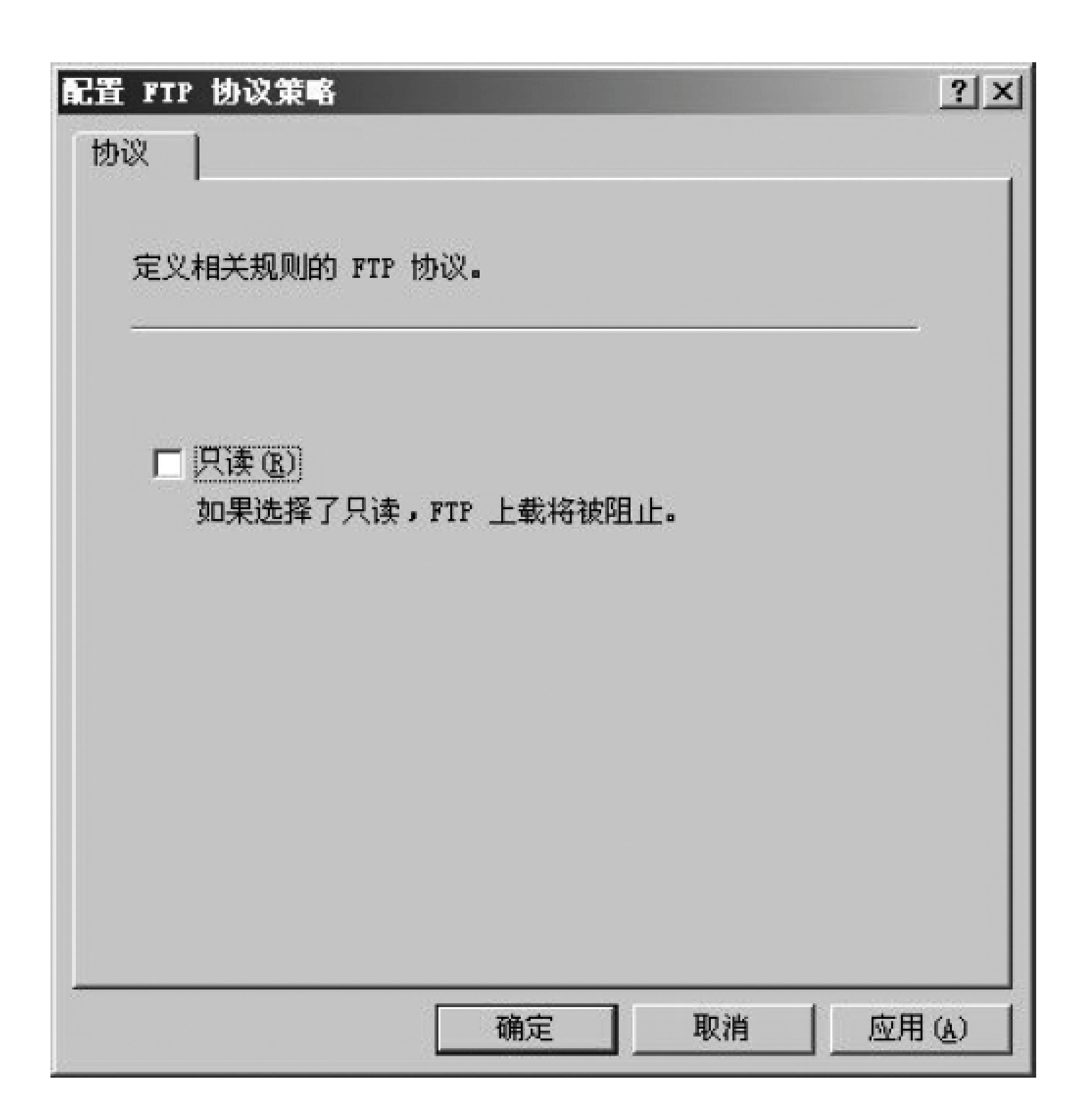


图 5-104 【配置 FTP 协议策略】对话框



图 5-105 新建协议

（2）在【欢迎使用新建协议定义向导】对话框中将此协议命名为 HTTP9988。

（3）在新建协议定义向导的【首要连接信息】对话框中，单击【新建】按钮，在打开的【新建/编辑协议连接】对话框中，【协议类型】下拉列表框中选择 TCP，【方向】下拉列表框中选择“出站”，端口范围的【从】文本框中和【到】文本框中都输入 9988，如图 5-106 所示。完成后单击【确定】按钮。

（4）在【辅助连接】对话框中直接单击【下一步】按钮。

（5）在【正在完成新建协议定义向导】对话框中单击【完成】按钮。

（6）回到【ISA 服务器管理】窗口，依次单击【应用】按钮、【确定】按钮。



完成新协议的创建后，就可以在访问规则内选用此协议，从用户定义的协议中选择刚才创建的新协议 HTTP9988，如图 5-107 所示。



图 5-106　新建/编辑协议连接



图 5-107　【添加协议】对话框

5.9　开放或阻挡实时通信软件

5.9.1　实时通信软件概述

常用的实时通信软件有腾讯 QQ、ICQ、微软 MSN 和移动 Fetion 等，这些实时通信软件虽然给人们提供一个非常方便的沟通方式，然而它们也带来了一些安全上的威胁，公司内部的重要数据也可能会轻易地通过实时通信软件传送出去。另外，如果公司内部员工在上班时间利用实时通信软件跟亲朋好友闲聊，也会降低员工的工作效率。

如果不让这些实时通信软件的流量通过 ISA Server 防火墙，虽然内部用户就没有机会跟亲朋好友闲聊，但同时也会无法跟客户、合作伙伴、供货商等通过实时通信软件来沟通，因此应该采用如下比较有效率的管理措施。

(1) 只针对公务上有需要使用实时通信软件的用户来开放，例如需要跟客户沟通的业务部员工。

(2) 只有特定时段开放，例如上班时段关闭，中午休息与下班时段才开放。

ISA Server 2006 默认并没有开放让内部的用户访问 Internet 的资源，因此默认时所有的实时通信与 P2P 软件流量都无法通过 ISA Server 防火墙。因此，为了开放或阻挡实时通信与 P2P 软件通过 ISA Server 防火墙，可以通过在 ISA Server 防火墙设置访问规则(防火墙策略)，打开或关闭某些特定端口来实现。常用的实时通信与 P2P 软件都有特定的端口，例如腾讯 QQ 使用端口是 4000、4001 和 8000，微软 MSN 使用的端口 1863、80、443 和 1080。本节以腾讯 QQ 为例说明如何通过 ISA Server 防火墙开放或阻挡实时通信与 P2P 软件。



5.9.2 开放或阻挡腾讯 QQ 测试环境

如图 5-108 所示，搭建开放或阻挡腾讯 QQ 通信的测试环境。

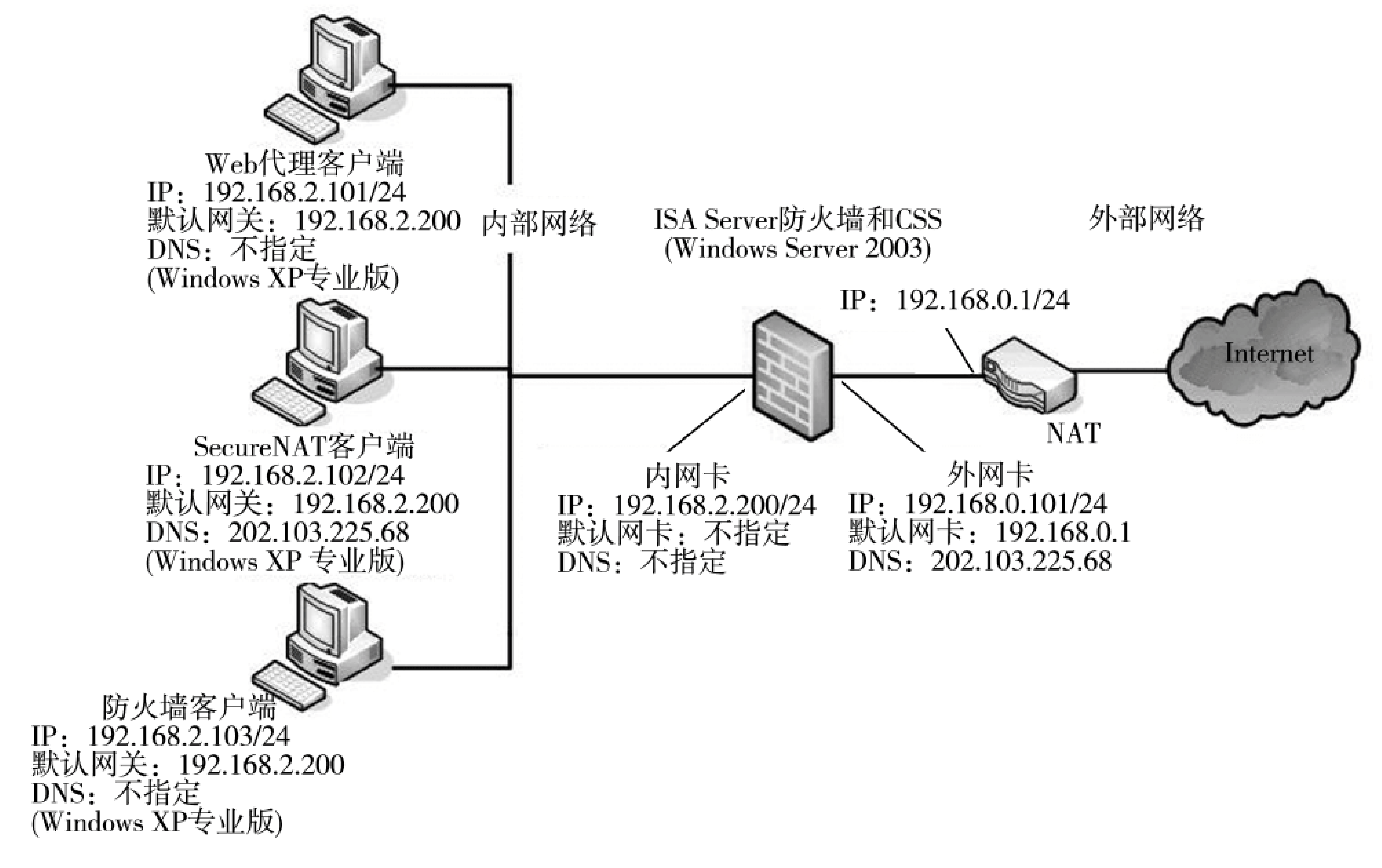


图 5-108　开放或阻挡腾讯 QQ 测试环境

注意：由于腾讯 QQ 通信的要求，在 Web 代理客户端和防火墙客户端的 IP 地址设置时需要给出默认网关(即 ISA Server 内网卡的 IP 地址 192.168.2.200)。

5.9.3 开放腾讯 QQ 实时通信步骤

1. 为 QQ 使用端口创建新协议

(1) 如图 5-109 所示，在【ISA 服务器管理】窗口的右边选择【工具箱】选项卡，选择【协议】/【新建】/【协议】命令，打开【新建协议定义向导】对话框。

(2) 在向导中出现【欢迎使用新建协议定义向导】对话框，在【协议定义名称】文本框中输入新建的协议的名称为“QQ 通信”，如图 5-110 所示。

(3) 单击【下一步】按钮，出现【首要连接信息】对话框，在该对话框中指定端口、协议以及方向，如图 5-111 所示。

(4) 单击【新建】按钮，出现【新建/编辑协议连接】对话框，在【协议类型】下拉列表中选择“UDP”，在【方向】下拉列表中选择“发送接收”，在【端口范围】文本框中指定 QQ 协议所使用的端口范围为 4000～4001，如图 5-112 所示。

(5) 单击【确定】按钮，返回【首要连接信息】对话框，并且设置 QQ 协议所使用的另外一个端口号为 8000，如图 5-113 所示。



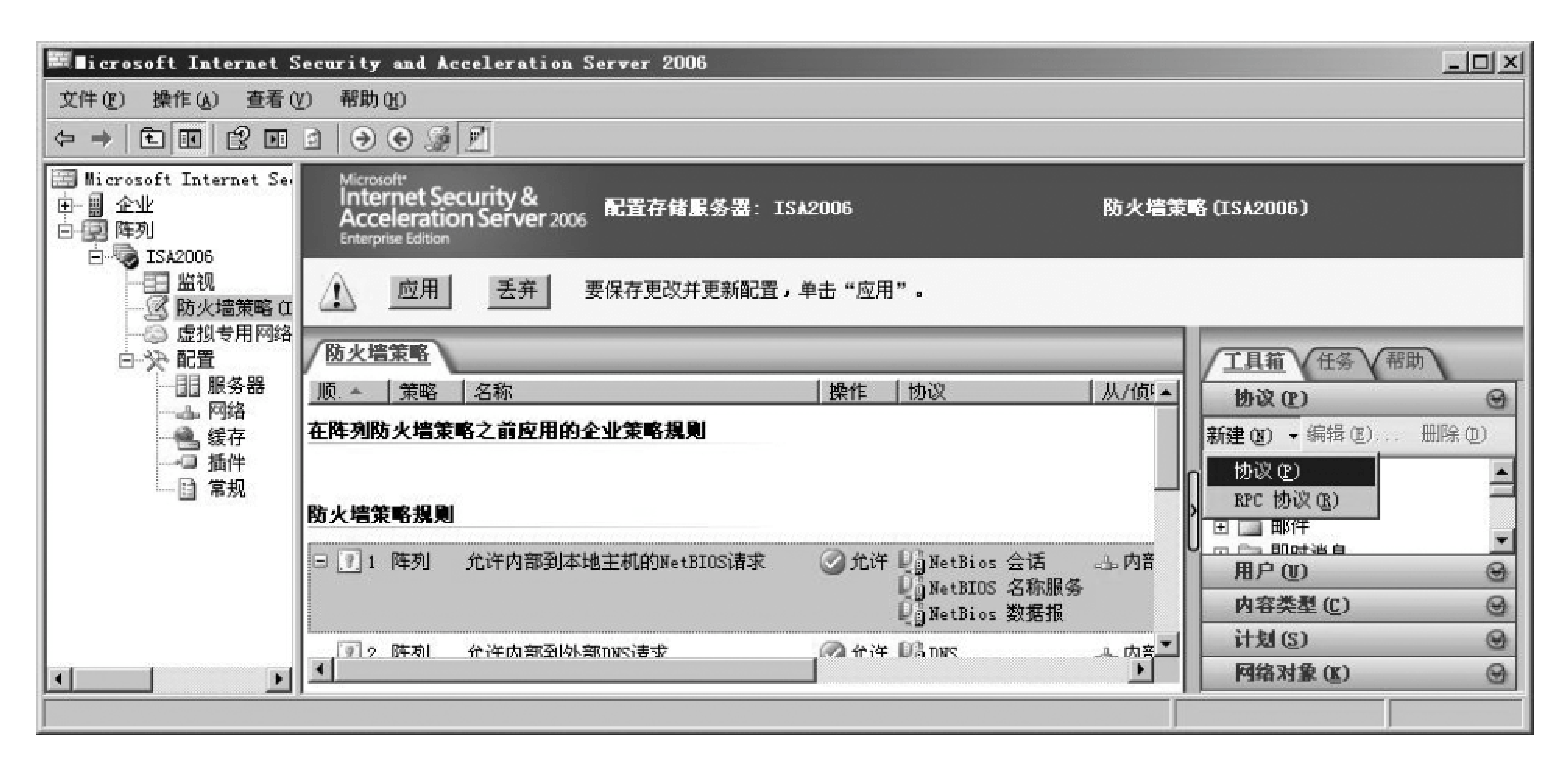


图 5-109　新建协议

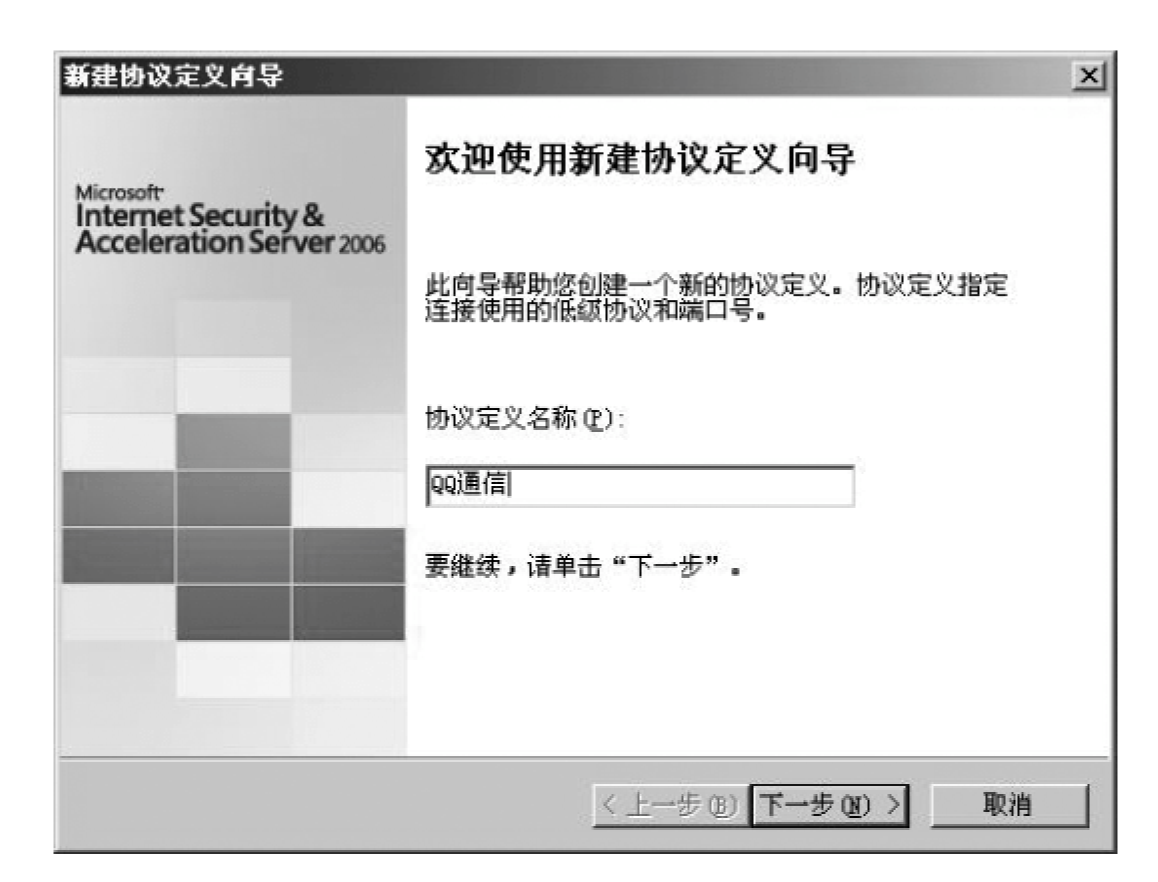


图 5-110　协议定义名称



图 5-111　【首要连接信息】对话框



图 5-112　添加 4000 到 4001 端口



图 5-113　添加另一个 8000 端口

（6）单击【确定】按钮，返回【首要连接信息】对话框，如图 5-114 所示，可以看到已经添加的端口范围、协议类型以及方向。

（7）单击【下一步】按钮，出现【辅助连接】对话框，如图 5-115 所示。单击此对话框的





【下一步】按钮，出现【正在完成新建协议定义向导】对话框，单击【完成】按钮即可。

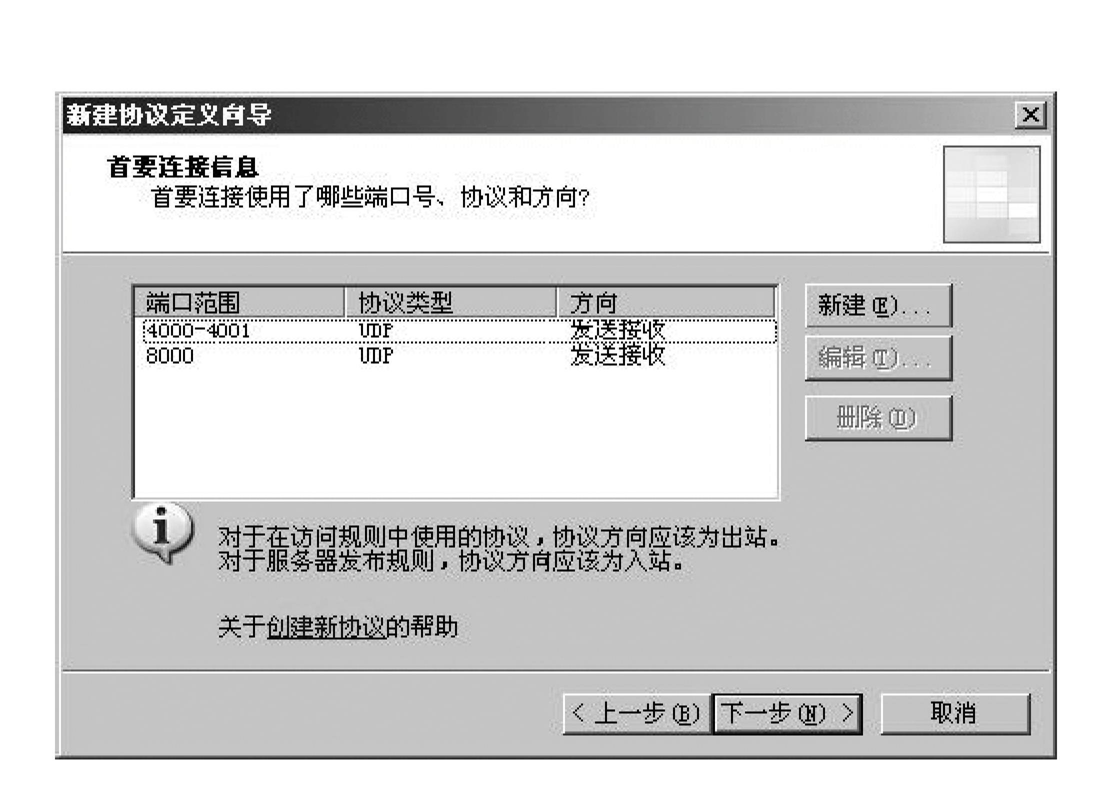




图 5-114 添加了端口后的对话框

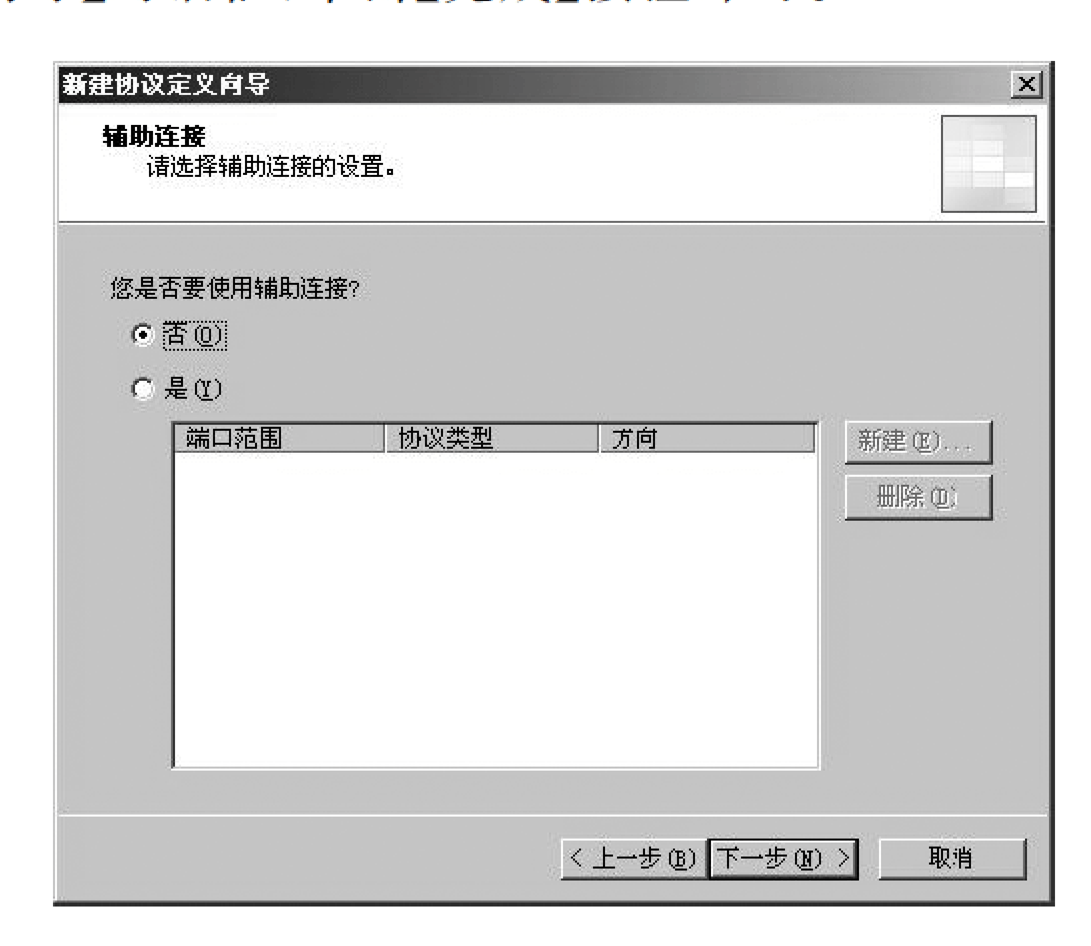


图 5-115 【辅助连接】对话框

(8) 返回【ISA 服务器管理】窗口，在【工具箱】选项卡区域的协议中可看到刚创建的协议，如图 5-116 所示。



图 5-116 新建【QQ 通信】协议

2. 创建 QQ 通信的访问规则(防火墙策略)

创建一个名称为"允许内部到外部的 QQ 通信"访问规则，创建的方法和步骤如 5.3 节所述。要注意的是，在【添加协议】对话框中选择协议时，应选择用户定义的"QQ 通信"协议，如图 5-117 所示。创建完成后，可以在【ISA 服务器管理】窗口中看见此访问规则，如图 5-118 所示。



图 5-117 【添加协议】对话框

3. 测试 QQ 通信

在客户端使用 QQ 登录，测试 QQ 是否能正常通信。





图 5-118 【允许内部到外部的 QQ 通信】访问规则

5.10 习 题

1. 简述 ISA Server 2006 的主要功能。
2. 简述 ISA 中的多网络结构。
3. 简述 ISA 支持的防火墙种类和网络模板。
4. ISA Server 2006 与其他软件防火墙相比,优势在哪里?
5. 简述使用 VMware Workstation 构建虚拟机的步骤。
6. 简述 ISA 中网络与网络集的含义。
7. 网络规则和防火墙访问规则是一样的吗? 区别在哪里?
8. 简述安装 ISA Server 2006 的过程。
9. 如何使用 ISA Server 2006 构建网页缓存服务器?
10. 对比三种 ISA Server 客户端,如何配置这三种客户端?
11. 简述在 ISA 防火墙中开放访问 Internet 的步骤。
12. 简述开放实时通信的步骤。



第6章　IDS与IPS

本章学习目标：

- 入侵检测系统模型及功能。
- 入侵检测系统的工作原理及分类。
- 常用入侵检测技术。
- 入侵防御系统的工作原理及分类。
- 防火墙、IDS 与 IPS 之间的关系。

通常，人们认为防火墙可以保护处于它身后的网络不受外界的侵袭和干扰。但随着网络技术的发展，网络结构日趋复杂，传统防火墙在使用的过程中暴露出以下的不足和弱点：入侵者可以伪造数据绕过防火墙或者找到防火墙中可能敞开的后门；防火墙不能防止来自网络内部的袭击，通过调查发现，将近 65％的攻击都来自网络内部；传统防火墙不具备对应用层协议的检查过滤功能，无法对 Web 攻击、FTP 攻击等做出响应；防火墙对于病毒蠕虫的侵袭也是束手无策。

因此，人们开始了对入侵检测系统（Intrusion-detection system，IDS）的研究及开发。IDS 与其他网络安全技术的不同之处在于，IDS 是一种积极主动的安全防护技术，是防火墙的有益补充，为网络提供实时的监控，并且在发现入侵的初期采取相应的防护手段。

然而，IDS 只能检测攻击，不能做到实时地阻止攻击，入侵防御系统（Intrusion-prevention system，IPS）填补了这个不足。IPS 是在应用层的内容检测基础上加上主动响应和过滤功能，填补了网络安全产品的基于内容的安全检查的空白。

6.1　入侵检测系统概述

IDS 是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全技术，是进行入侵检测的软件与硬件的组合。我们做一个形象的比喻：假如防火墙是一幢大楼的门卫，那么 IDS 就是这幢大楼里的监视系统。一旦非法人员进入大楼，或内部人员有越界行为，只有实时监视系统才能发现情况并发出警告。

6.1.1　入侵检测系统的功能

一个成功的 IDS 不但可以使系统管理员时刻了解网络系统（包括程序、文件和硬件设



备等)的任何变更,还能给制定网络安全策略提供指导。更为重要的一点是,它应该管理、配置简单,从而使非专业人员能非常容易地获得网络安全。而且,入侵检测的规模还应根据网络威胁、系统构造和安全需求的改变而改变。IDS在发现入侵后,会及时做出响应,包括切断网络连接、记录事件和报警等。因此,IDS通常具有以下功能:

- 监视用户和系统的运行状况,查找非法用户和合法用户的越权操作。
- 对系统的构造和弱点进行审计。
- 识别分析著名攻击的行为特征并报警。
- 对异常行为模式进行统计分析。
- 评估重要系统和数据文件的完整性。
- 对操作系统进行跟踪审计管理,并识别用户违反安全策略的行为。
- 容错功能。即使系统发生崩溃,也不会丢失数据,或者系统重新启动时重建自己的信息库。

6.1.2　入侵检测系统的模型

为了提高IDS产品、组件及与其他安全产品之间的互操作性,美国国防高级研究计划署(The U.S. Defense Advanced Research Projects Agency,DARPA)和互联网工程任务组(Internet Engineering TaskForce,IETF)的入侵检测工作组(Intrusion Detection working Group,IDWG)发起制定了一系列建议草案,从体系结构、API、通信机制、语言格式等方面规范IDS的标准。DARPA提出的建议是公共入侵检测框架(Common Intrusion Detection Framework,CIDF)。CIDF提出了一个通用模型,将入侵检测系统分为4个基本组件:事件产生器、事件分析器、事件响应单元和事件数据库,其结构如图6-1所示。

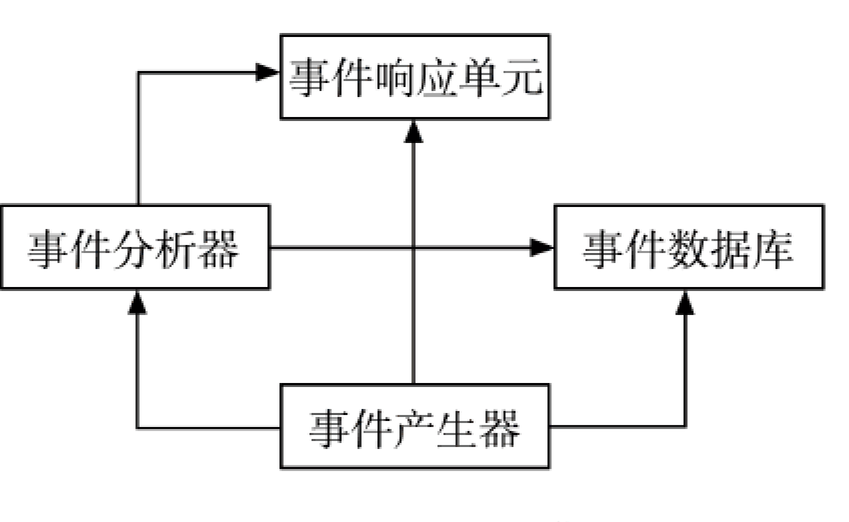


图6-1　CIDF的模型

1. 事件产生器

CIDF将IDS需要分析的数据统称为事件,事件既可以是网络中的数据包,也可以是从系统日志或其他途径得到的信息。事件产生器(Event Generators)的任务是从入侵检测系统之外的计算环境中收集事件,并将这些事件转换成CIDF的GIDO(Generalized Intrusion Detection Objects,统一入侵检测对象)格式传送给其他组件。

2. 事件分析器

事件分析器(Event Analyzers)分析从其他组件收到的GIDO,并将产生的新GIDO再传送给其他组件。分析器可以是一个轮廓(profile)描述工具,统计性地检测现在的事件是否可能与以前某个时间来自同一个时间序列;也可以是一个特征检测工具,用于在一个事件序列中检测是否有已知的误用攻击特性。此外,事件分析器还可以是一个相关器,观察事件之间的关系,将有联系的事件放在一起,以利于以后的进一步分析。



3. 事件数据库

事件数据库(Event Databases)用来存储GIDO,以备系统需要的时候使用。

4. 事件响应单元

事件响应单元(Response Units)处理收到的GIDO,并据此采取相应的措施,如相关进程、将连接复位、修改文件权限等。

在这个模型中,事件产生器、事件分析器和响应单元通常以应用程序的形式出现,而事件数据库则往往是文件或数据流的方式。

以上4个组件只是逻辑实体,一个组件可能是某台计算机上的一个进程甚至线程,也可能是多台计算机上的多个进程,它们以GIDO格式进行数据转换。GIDO是对事件进行编码的标准通用格式(由CIDF描述语言CISL定义),GIDO数据流在图中已标出,它可以是发生在系统中的审计事件,也可以是对审计事件的结果分析。

6.1.3 入侵检测技术及其发展趋势

1. 入侵检测技术

入侵检测技术是为保证计算机网络系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术,是一种用于检测计算机中违反安全策略行为(非法用户的违规行为——入侵,合法用户的违规行为——滥用)的技术。

从具体的检测理论来看,IDS的检测分析技术主要有误用检测技术和异常检测技术两大类。大部分现有的入侵检测工具都使用误用检测技术。异常检测技术虽然还没有得到广泛应用,但很多人认为,异常检测在未来的IDS中将有很大的发展。

(1) 误用检测技术。误用检测技术应用了系统缺陷和特殊入侵的累积知识,因此误用检测也称为基于知识的检测技术或模式匹配检测技术。

误用检测技术假定所有的入侵行为和手段都能够表达一种模式或特征。如果将以往发现的所有网络攻击的特征总结出来,并建立一个入侵信息库,则IDS可以将当前捕获到的网络行为特征与入侵信息库中的特征信息相比较,如果匹配,则当前行为就被认定是入侵行为。

误用检测技术具有检测准确度高、技术相对成熟、便于进行系统防护等优点,但它也有入侵信息的收集和更新困难、难以检测本地入侵和新的入侵行为、维护特征库的工作量巨大等缺点。误用检测技术的实现主要有专家系统、特征分析、条件概率、键盘监控、模型推理和状态转换分析等方法。

(2) 异常检测技术。异常检测技术又称为基于行为的入侵检测技术,是指根据用户的行为和系统资源的使用状况判断是否存在入侵。

异常检测技术首先假定网络攻击行为是不常见的或异常的,区别于所有的正常行为。如果能够为用户和系统的所有正常行为总结活动规律并建立行为模型,那么IDS可以将当前捕获到的网络行为与行为模型进行比较,若入侵行为偏离了正常行为轨迹,就可以被检测

出来。

异常检测的优点是能够检测出新的入侵或从未发生过的入侵；对操作系统的依赖性较小；可检测出属于滥用权限型的入侵。其缺点是报警率高和行为模型建立困难。异常检测技术的实现主要有概率统计、特征选择、贝叶斯推理、贝叶斯网络、贝叶斯聚类、神经网络、模式预测、数据采掘和人工免疫等方法。

2．入侵检测技术的发展趋势

随着 Internet 的发展与广泛应用，无论从规模与方法上，网络入侵的手段与技术也都有了"进步与发展"。入侵技术的发展主要反映出入侵的复杂化、间接化、规模的扩大化、技术的分布化等。根据这些特点，今后的入侵检测技术大致可向以下几个方向发展。

- 分布式入侵检测：传统的 IDS 局限于单一的主机或网络架构，对异构系统及大规模的网络检测明显不足，不同的 IDS 系统之间不能协同工作。为解决这一问题，需要发展分布式入侵检测技术与通用入侵检测架构。
- 智能化入侵检测：即使用智能化的方法与手段来进行入侵检测。现阶段常用的智能化方法有神经网络、遗传算法、模糊技术、专家系统、免疫原理等，这些方法常用于入侵特征的辨识。
- 全面的安全防御方案：使用安全工程风险管理的思想与方法来处理网络安全问题，从管理、网络结构、加密通道、防火墙、病毒防护、入侵检测多方位地对所关注的网络作全面评估，然后提出可行的全面解决方案。
- 分析技术的改进：采用当前的分析技术和模型，会产生大量的误报和漏报，难以确定真正的入侵行为。采用协议分析和行为分析等新的分析技术后，可极大地提高检测效率和准确性，从而对真正的攻击做出反应。协议分析技术是在对网络数据流进行重组的基础上，理解应用协议，再利用模式匹配和统计分析的技术来判明攻击；行为分析技术不仅分析单次攻击事件，还根据前后发生的事件确认是否有攻击发生、攻击行为是否生效，是入侵检测分析技术的最高境界。
- 向高度可集成性发展：未来的 IDS 将会结合其他网络管理软件，形成入侵检测、网络管理、网络监控三位一体的工具。

6.1.4　入侵检测的流程

入侵检测系统的检测流程包括两个步骤：信息收集和信息分析。

1．信息收集

入侵检测很大程度上依赖于所收集信息的可靠性和正确性，因此，有必要利用所掌握的真正的和精确的软件来报告这些信息。因为黑客经常采用替换的方法以篡改这些信息，例如替换被程序调用的子程序、库和其他工具。举例来说，UNIX 系统的 PS 指令可以被替换为一个不显示入侵过程的指令，或者是编辑器被替换成一个读取不同于指定文件的文件。因此，需要保证用来检测网络系统的软件的完整性，特别是入侵检测系统本身应具有足够的坚固性，以防止被篡改而收集到错误的信息。



入侵检测利用的信息一般来自以下 4 个方面。

(1) 系统和网络日志文件。黑客经常在系统日志文件中留下他们的踪迹,因此,充分利用系统和网络日志文件信息是检测入侵的必要条件。日志中包含发生在系统和网络上的不寻常和不期望活动的证据,这些证据可以指出有人正在入侵或已成功入侵了系统。通过查看日志文件,能够发现成功的入侵或入侵企图,并可以很快地启动应急响应程序。

(2) 非正常的系统目录和文件改变。网络环境中的文件系统包含很多软件和数据文件,包含重要信息的文件和私有数据文件经常是黑客修改或破坏的目标。目录和文件中的不期望的改变(包括修改、创建和删除),特别是那些正常情况下限制访问的目录或文件,很可能是一种入侵产生的指示和信号。

(3) 非正常的程序执行。网络系统上的程序执行一般包括操作系统、网络服务、用户启动的程序和特定目的的应用。每个在系统上执行的程序由一到多个进程来实现,每个进程执行在具有不同权限的环境中,这种环境控制着进程可访问的系统资源、程序和数据文件等。一个进程的执行行为由它运行时执行的操作来表现,操作执行的方式不同,它利用的系统资源也就不同。一个进程出现了不期望的行为可能表明黑客正在入侵你的系统。

(4) 物理形式的入侵信息。这包括两方面的内容:一是未授权的网络硬件连接;二是对物理资源的未授权访问。黑客可以知道网上由用户添加的不安全(未授权)设备,然后利用这些设备访问网络。例如,用户在家里可能安装 Modem 以访问远程办公室,与此同时黑客正在利用自动工具来识别在公共电话线上的 Modem,如果拨号访问的数据流经过这些自动工具,那么这一拨号访问就成了威胁网络安全的后门,黑客就会利用这个后门访问内部网,从而越过内部网络原有的防护措施,然后捕获网络流量,进而攻击其他系统,窃取敏感信息等。

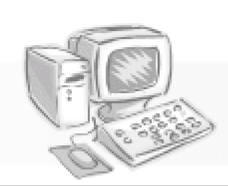
2. 信息分析

对上述 4 类收集到的有关系统、网络、数据及用户活动的状态和行为等信息,一般通过 3 种技术手段进行分析:模式匹配、统计分析和完整性分析。其中前两种方法用于实时的入侵检测,而完整性分析则用于事后分析。

(1) 模式匹配。模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较,从而发现违背安全策略的行为。该方法的一大优点是只需收集相关的数据集合,且技术已相当成熟。它与杀毒软件、防火墙采用的方法一样,检测准确率和效率都相当高。但是,该方法存在的弱点是需要不断地升级以对付不断出现的黑客攻击手法,不能检测到从未出现过的黑客攻击手段。

(2) 统计分析。统计分析方法首先给系统对象(如用户、文件、目录和设备等)创建一个统计描述,统计正常使用时的一些测量属性(如访问次数、操作失败次数和延时等)。测量属性的平均值将被用来与网络、系统的行为进行比较,当观察值在正常值范围之外时,就认为有入侵行为发生。其优点是可检测到未知的入侵和更为复杂的入侵,缺点是误报、漏报率高,且不适应用户正常行为的突然改变。

(3) 完整性分析。完整性分析主要关注某个文件或对象是否被更改,包括文件和目录的内容及属性,它在发现被更改的、被植入木马的应用程序方面特别有效。完整性分析利用强有力的加密机制(例如 MD5),因而它能识别哪怕是微小的变化。其优点是不管模式匹



配方法和统计分析方法能否发现入侵，只要是成功的攻击导致了文件或其他对象的任何改变，它都能够发现。缺点是一般以批处理方式实现，不能用于实时响应。

6.2　入侵检测系统的分类

如果按照检测对象划分，入侵检测技术又可分为基于主机的入侵检测系统、基于网络的入侵检测系统和混合型入侵检测系统 3 大类。下面分别予以简单介绍。

6.2.1　基于主机的入侵检测系统

基于主机的入侵检测系统（Host Intrusion Detection System，HIDS）的输入数据来源于系统的审计日志，即在每个要保护的主机上运行一个代理程序，一般只能检测该主机上发生的入侵，基于主机的入侵检测系统一般在重要的系统服务器、工作站或用户机器上运行，监视操作系统或系统事件的可疑活动，寻找潜在的可疑活动（如尝试登录失败）。此类系统需要定义清楚哪些是不合法的活动，然后把这种安全策略转换成入侵检测规则。

1. 主机入侵检测系统的优点

主机入侵检测系统对分析“可能的攻击行为”非常有用。举例来说，有时候它除了指出入侵者试图执行一些“危险的命令”之外，还能分辨出入侵者干了什么事、他们运行了什么程序、打开了哪些文件、执行了哪些系统调用。主机入侵检测系统与网络入侵检测系统相比通常能够提供更详尽的相关信息，误报率更低。

2. 主机入侵检测系统的弱点

主机入侵检测系统安装在需要保护的设备上，全面部署代价较大，而且降低了应用系统的效率。此外，它将本来不允许安全管理员有权访问的服务器变成可以访问。

主机入侵检测系统的另一个问题是它依赖于服务器固有的日志与监视能力。

主机入侵检测系统除了监测自身的主机以外，根本不监测网络上的情况。对入侵行为的分析工作量将随着主机数目增加而增加。

6.2.2　基于网络的入侵检测系统

基于网络的入侵检测系统（Network Intrusion Detection System，NIDS）的输入数据来源于网络的信息流，该类系统一般被动地在网络上监听整个网络上的信息流，通过捕获网络数据包，进行分析，检测该网段上发生的网络入侵，如图 6-2 所示。

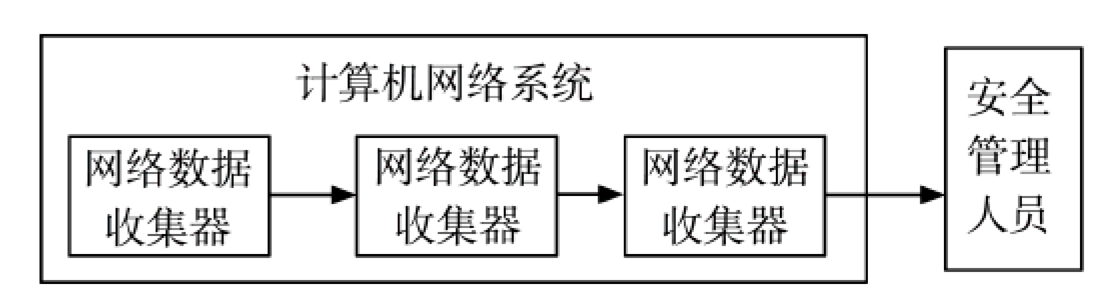


图 6-2　基于网络的入侵检测过程



1. 网络入侵检测系统的优点

网络入侵检测系统能够检测那些来自网络的攻击，能够检测到超过授权的非法访问。

网络入侵检测系统不需要改变服务器等主机的配置。由于它不会在业务系统的主机中安装额外的软件，从而不会影响系统的性能。

由于网络入侵检测系统不像路由器、防火墙等关键设备那样工作，因此它不会成为系统中的关键路径。由于网络入侵检测系统发生故障不会影响正常业务的运行，因此部署一个网络入侵检测系统的风险比主机入侵检测系统的风险少得多。

2. 网络入侵检测系统的弱点

网络入侵检测系统只检查它直接连接网段的通信，不能检测在不同网段的网络包。而安装多台网络入侵检测系统会使成本大大增加。

网络入侵检测系统为了提高性能通常采用特征检测的方法，它可以检测出一些普通的攻击，而很难检测一些复杂的需要大量计算与分析时间的攻击。

网络入侵检测系统可能会将大量的数据传回分析系统中，产生大量的分析数据流量。

6.2.3 混合型入侵检测系统

基于网络的入侵检测产品和基于主机的入侵检测产品都有不足之处，单纯使用其中一类产品会造成主动防御体系不全面。由于两者的优缺点可以互补，如果将它们无缝地结合起来部署在网络内，则会构架成一套完整的、立体的主动防御体系。综合了基于网络的和基于主机的两种结构特点的 IDS，既可发现网络中的攻击信息，也可从系统日志中发现异常情况。

完美的 IDS 产品应该将两者结合起来，一些高端的 IDS 产品都采用 HIDS 和 NIDS 有机结合的混合型 IDS 架构。

6.3 典型入侵检测产品介绍

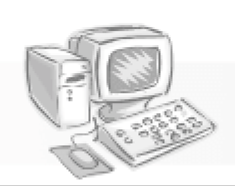
6.3.1 金诺网安入侵检测系统 KIDS

金诺网安入侵检测系统 KIDS 是上海金诺网络安全技术股份有限公司自主研发的入侵检测系统，是国家“863”安全应急计划课题的延伸和发展。

金诺网安入侵检测系统 KIDS 将主机入侵检测和网络入侵检测相结合，分别从计算机和网络的各个关键点收集违反安全策略的行为和被攻击的迹象，并且可以根据用户的需要实时报警和响应。金诺网安入侵检测系统既可以防止来自外网的黑客入侵，也可以制止来自内网的恶意行为、误操作和资源滥用，提高了信息安全基础结构的完整性。

1. KIDS 的模块组成

KIDS 检测系统具有非常丰富的功能模块，全面地为入侵检测服务。



(1) 管理中心。作为系统中心的KIDS管理中心(KIDS Management Center,KMC)包含大部分的功能组件:控制台、事件处理器、响应器、策略编辑器、数据库管理工具和报表分析工具等。KMC可以安装在Windows平台上。KMC的结构如图6-3所示。

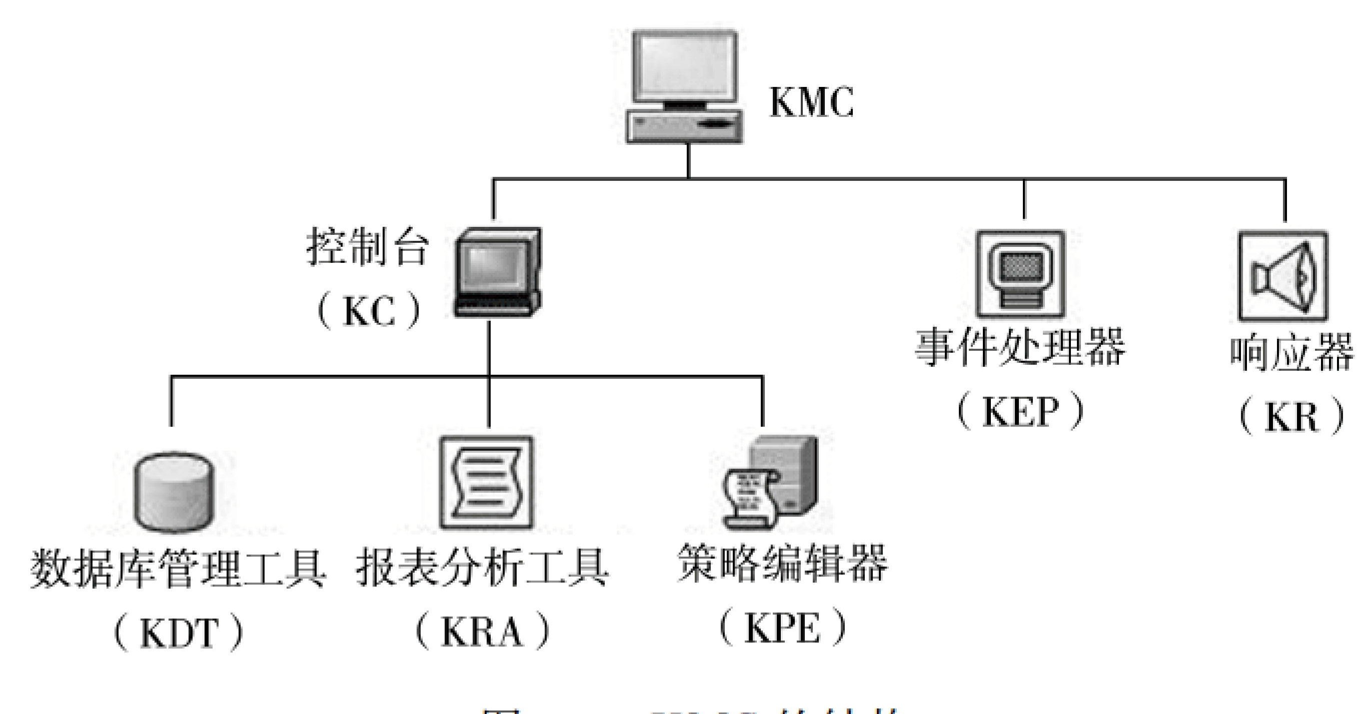


图6-3 KMC的结构

(2) 控制台。控制台(KIDS Console,KC)提供了日常使用的用户界面,可以管理各组件和监视警报及审计信息,并可以调用各类工具。KC包含数据库管理(KDT)、报表分析(KEA)和策略编辑器(KPE)等工具。

(3) 事件处理器。事件处理器(KIDS Event Processor,KEP)接收来自传感器的事件,根据策略记录到数据库中、分发到控制台、分发到上级事件处理器或分发到响应器中。

(4) 数据库管理工具。数据库管理工具(KIDS Database Tool,KDT)是对KIDS数据库进行管理和维护的主要工具,通过KDT,用户可以实现对数据库进行备份、合并或删除等具体操作。

(5) 策略编辑器。策略编辑器(KIDS Policy Editor,KPE)是定义KIDS系统检测策略和响应策略等内容的功能组件,策略编辑器会形成相应的配置文件为系统调用。

(6) 响应器。响应器(KIDS Responder,KR)主要产生响应动作,如阻断、关闭系统和产生各类报警等。

(7) 报表分析工具。报表分析工具(KIDS Reporter and Analyzer,KRA)是对KIDS数据库中的报警日志进行统计分析的重要工具,可以为用户提供详细的明细报表和各类图文并茂的统计报表,并实现入侵分析和对安全进行评估的目的。

2. KIDS的主要功能

(1) 识别各种黑客攻击或入侵的方法和手段。

(2) 监控内部人员的误操作、资源滥用或恶意行为。

(3) 实时的报警和响应,帮助用户及时发现并解决安全问题。

(4) 核查系统漏洞及后门。

(5) 协助管理员加强网络安全管理。

借助KIDS系统,网络管理人员可以随时了解人们正在访问的信息,并且在有人试图偷窥或盗取敏感数据时及时觉察。



6.3.2 华强 IDS

1. 华强 IDS 组成

华强入侵检测系统是一套基于网络的分布式入侵检测系统，主要由两个部分组成：响应控制台和探测引擎，是一套软、硬件结合的入侵检测系统。

(1) 探测引擎。探测引擎是安装在计算机局域网上的物理设备，它可以同时监控两个网段，它的主要功能是采集网络上的数据包信息，按照设定的规则过滤出相关的数据，对于入侵或非法登录实时报警或切断，同时向监控中心发送报警信息。

探测引擎是华强入侵检测系统运行的核心，它监听该引擎所在的物理网络上的所有通信信息，分析这些网络通信信息，将分析结果与探测引擎上运行的策略集相匹配，依照匹配结果对网络信息的交换执行报警、阻断及记录日志等功能。同时它还需要完成对控制中心指令的接收和响应工作。

(2) 响应控制台。控制台是一套运行于 Windows 系列操作系统上的高性能、智能化的管理系统，集中管理本地或远程网段的多个探测引擎，以动态的扫描界面显示各引擎所监控网段内的每台主机。当发现入侵行为时，它以动态的方式显示具体受入侵的主机位置，并且详细显示入侵告警信息，包括源 IP 地址、端口，目的 IP 地址和端口以及攻击特征等信息。

2. 华强 IDS 的应用

对于不同的网络结构和应用目的，华强入侵检测系统的安装方式和策略配置会有所不同。如图 6-4 所示的是该系统在简单集线器或交换机网络中的网络拓扑。建议将华强入侵检测系统与防火墙配套使用，并结合网络安全扫描系统，构建安全的、全面的网络拓扑。如图 6-5 所示的是华强入侵检测系统在用户中应用的一般网络结构图。

从图 6-4 所示的网络结构中可以看出，在一般的小型网络中，只需部署单个 IDS 系统即可，因为整个网络比较简单，检测策略都基本一样。但在比较复杂的大中型企业网络中，就需要在不同网段或者不同检测策略的网段分别部署一套 IDS 系统，以满足不同检测需求。如图 6-5 所示，在分别位于主网络区域、应用服务器区域和防火墙 DMZ 区域的公用服务器系统中肯定有不同的检测策略，这样就得分别部署配置不同策略的 IDS 系统了。

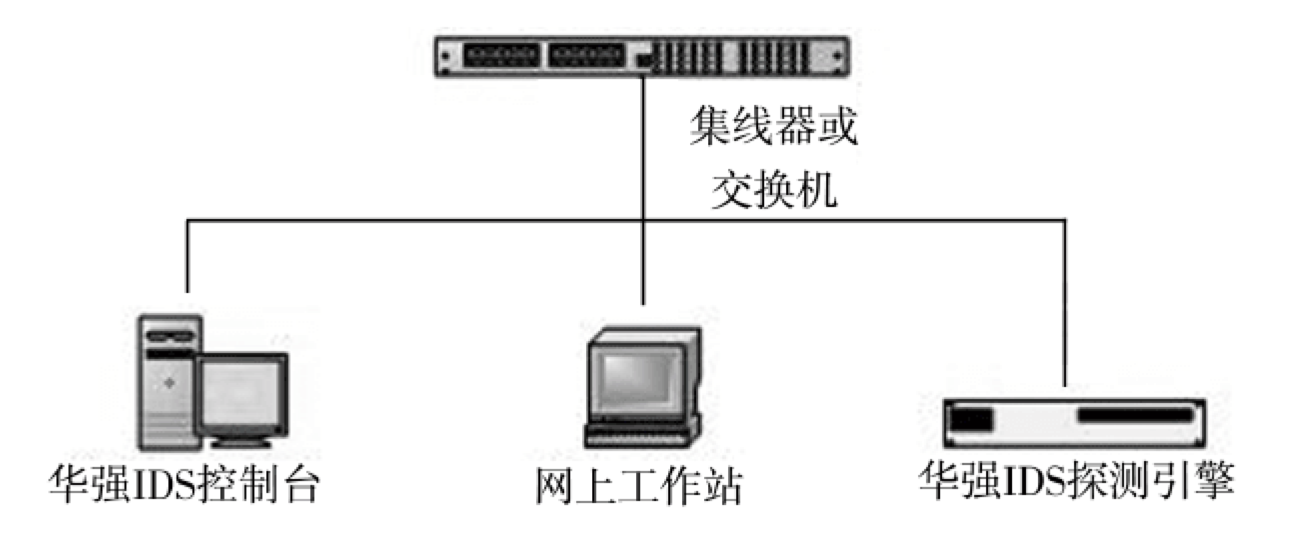


图 6-4　华强 IDS 的基本应用网络结构图





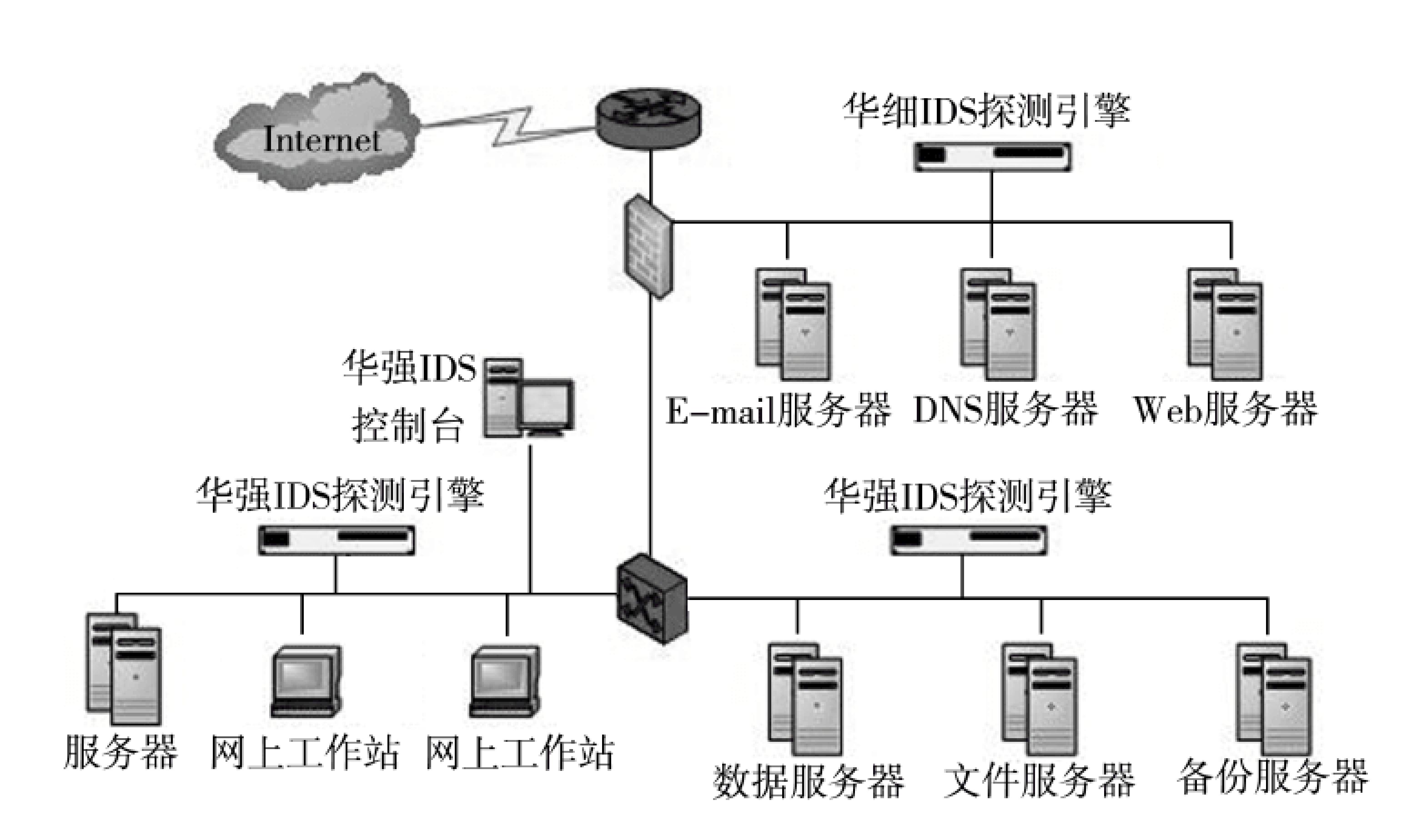


图 6-5 华强 IDS 应用方案的一般结构图

6.3.3 黑盾网络入侵检测系统

黑盾网络入侵检测系统(HD-NIDS)是福建省海峡信息技术有限公司自行研制开发的分布式网络入侵检测软件系统。HD-NIDS 是采用国际上先进的分布式入侵检测理论构架的高智能分布式入侵检测系统。其强有力的分布式 Agent 分散在每一个子网的旁路,全天候 24 小时监视各个子网络的通信情况,及时捕获入侵和攻击行为,并予以报警、记录及实时响应。

HD-NIDS 代表着最新一代的网络安全技术,不仅具有基本的入侵侦测能力,更拥有国际上最先进的反 IDS 欺骗技术和反 IDS flood 技术,可以成功地将种种变形和欺骗一一捕获。

1. HD-NIDS 的功能

HD-NIDS 不仅使系统管理员实时了解网络系统(包括程序、文件和硬件设备等)的任何变更,还能给网络安全策略的制定提供依据。更为重要的一点是它属于一种动态安全技术(主动防御)范畴,是一种管理方便、配置简单的网络防御技术,可以使非专业人员非常容易地掌握操作技巧,确保网络安全。HD-NIDS 主要包括以下功能模块。

- 网络实时检测功能:以流量柱状或流量线性图表示网络流量、协议流量、用户流量和不同包长度的流量分布。
- 内容过滤功能:用户能够根据自定义的关键字进行告警、阻断诸如网页、FTP 等应用中出现的明文编码。
- MAC-IP 绑定:根据预定义好的 MAC-IP 对应列表,发现非法使用别人 IP 的用户,并可以选择加以阻断。
- 页面重组功能:HD-NIDS 可以将信息网络中的 Telnet、FTP、HTTP、POP3、SMTP 或其他用户定义的任意服务的通信过程记录下来,并将所有数据内容进行回放,在监控台实现页面重组。
- 主机多网卡配置:在大型网络中主机多网卡是相当常见的。通常多网卡的主机一般同时跨多个网段。HD-NIDS 利用独特的 Spider 技术,可以同时监控多网卡主机



所在的多个网段。

- 定义规则：系统默认提供了上千条最新的黑客规则，并可以对规则进行自动升级。用户可以自定义或编辑规则，可以决定是否使用它。
- 自动扫描网络状态：可以自动扫描局域网主机信息，并将得到的信息应用到 NIDS 引擎中，这样可以防止黑客的无效攻击，可以智能高效地实现一个安全网络。
- 阻断功能：对符合系统或用户定义的黑客规则的数据包可以进行阻断；对某个占网络流量过大的用户可以进行阻断；对不符合 MAC-IP 绑定的数据包可以进行阻断。
- log 查询功能：可以使用 MS SQL Server 或文本文件存放 log，并提供详尽的 log 查询。
- 查询模块：HD-NIDS 记录数据包可以基于数据库模块查询，也可以基于文件存储查询。
- 在线升级功能：HD-NIDS 及时更新黑客入侵特征库，正式用户能将 HD-NIDS 在线升级到最新版本。

2. HD-NIDS 的网络应用

在内部网络中各主机使用共享式 Hub 连接到交换机上，或主机直接连接到交换机上，交换机再通过路由器接入外部网络。为了使 HD-NIDS 检测到受保护网络（主机）的所有通信，必须将 HD-NIDS 监控系统接到交换机的监听口上，也可以把 HD-NIDS 接到所要监听的网段所在的共享式集线器上。如图 6-6 所示是 HD-NIDS 的简单网络应用示意图。

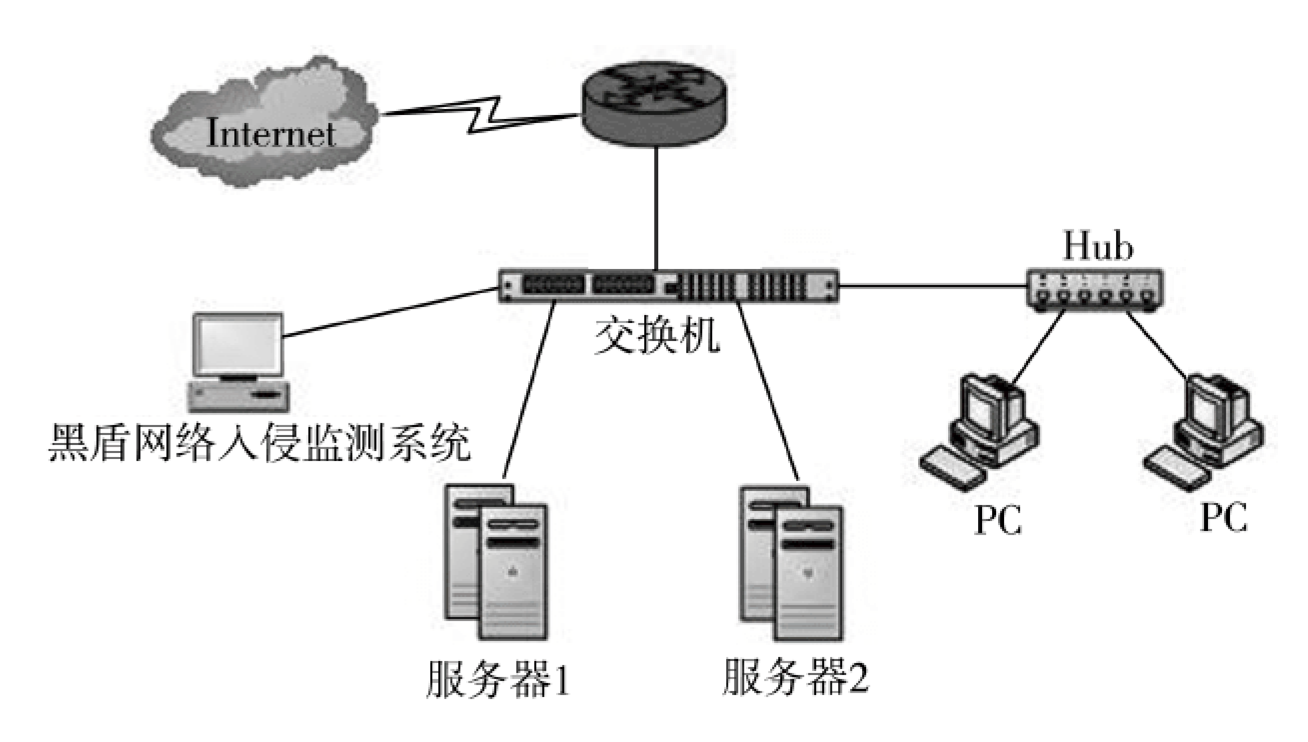


图 6-6　黑盾网络入侵检测系统的简单网络应用示意图

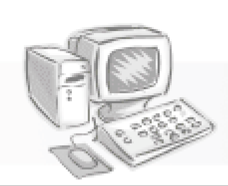
HD-NIDS 除了可应用于简单的内部网络中，还可应用于网络分布较复杂的环境中。在这种分布式网络环境中，内部网络中各个部门通过从交换机连接到主交换机上，再通过主交换机连接路由器接入因特网或外部网络。

6.4　萨客嘶入侵检测系统

6.4.1　萨客嘶入侵检测系统介绍

1. 萨客嘶入侵检测系统概述

萨客嘶入侵检测系统是一种积极主动的网络安全防护工具，提供了对内部和外部攻击的实时保护，它通过对网络中所有传输的数据进行智能分析和检测，从中发现网络或



系统中是否有违反安全策略的行为和被攻击的迹象,在网络系统受到危害之前拦截和阻止入侵。

萨客嘶入侵检测系统基于协议分析,采用了快速的多模式匹配算法,能对当前复杂高速的网络进行快速精确分析,在网络安全和网络性能方面提供全面和深入的数据依据,是企业、政府、学校等网络安全立体纵深、多层次防御的重要产品。

2. 萨客嘶入侵检测系统主要功能

(1) 入侵检测及防御功能。检测用户网络中存在的黑客入侵、网络资源滥用、蠕虫攻击、后门木马、ARP欺骗、拒绝服务攻击等各种威胁。同时可以根据策略配置主动切断危险行为,对目标网络进行保护。

(2) 行为审计功能。对网络中用户的行为进行审计记录,包括用户范围Web网站,收发邮件,使用FTP传输文件,使用MSN、QQ等即时通信软件等行为,帮助管理员发现潜在的网络威胁。同时对网络中的敏感行为进行审计。

(3) 流量统计功能。对网络流量进行实时显示和统计分析,帮助用户有效地发现网络资源滥用、蠕虫、拒绝服务攻击,确保用户网络正常使用。

(4) 策略自定义功能。高级用户可以根据自身网络情况,对检测规则进行定义,制定针对用户网络的高效策略,加强入侵检测系统的检测准确性。

(5) 警报响应功能。对警报事件进行及时响应,包括实时切断会话连接、记录日志。

(6) IP碎片重组。利用碎片穿透技术突破防火墙和欺骗IDS已经成为黑客们常用的手段,萨客嘶入侵检测系统能够进行完全的IP碎片重组,发现所有的基于IP碎片的攻击。

(7) TCP状态跟踪及流重组。通过对TCP协议状态的跟踪,能够完全避免因单包匹配造成的误报。Stick、Snot等黑客工具通过发送没有经过三次握手的TCP攻击报文触发大量的IDS报警,但这些TCP报文并不会真正对目标机器产生实际的效果(通常是被丢弃)。此时IDS产生大量的警告就属于误报。处理不当可能造成IDS系统瘫痪。萨客嘶入侵检测系统完全模仿受保护的机器丢弃这些残缺报文,极大地减小了误报率。

采用类似于Telnet方式将攻击报文拆成一个个的小报文进行发送,可以逃避基于单包的IDS的检测。萨客嘶入侵检测系统采用流汇重组式检测该类攻击手段。

6.4.2 萨客嘶入侵检测步骤

实施萨客嘶入侵检测需要在一台Windows 2000/XP的计算机上安装萨客嘶入侵检测系统,还需要在另一台作为入侵扫描用途的计算机上安装扫描软件,以便对目标主机进行扫描。详细步骤如下。

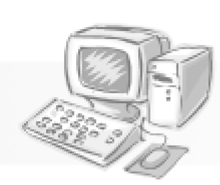
1. 在192.168.0.21上运行Nmap,对目标主机(192.168.0.20)进行扫描

(1) 在Command(命令)栏输入命令:nmap-sS 192.168.0.20

扫描探测到目标主机上四个开放端口21、139、445和1110(图6-7)

(2) 在Command栏输入命令:nmap-O 192.168.0.20

扫描探测到目标主机的操作系统类型,如图6-8所示。



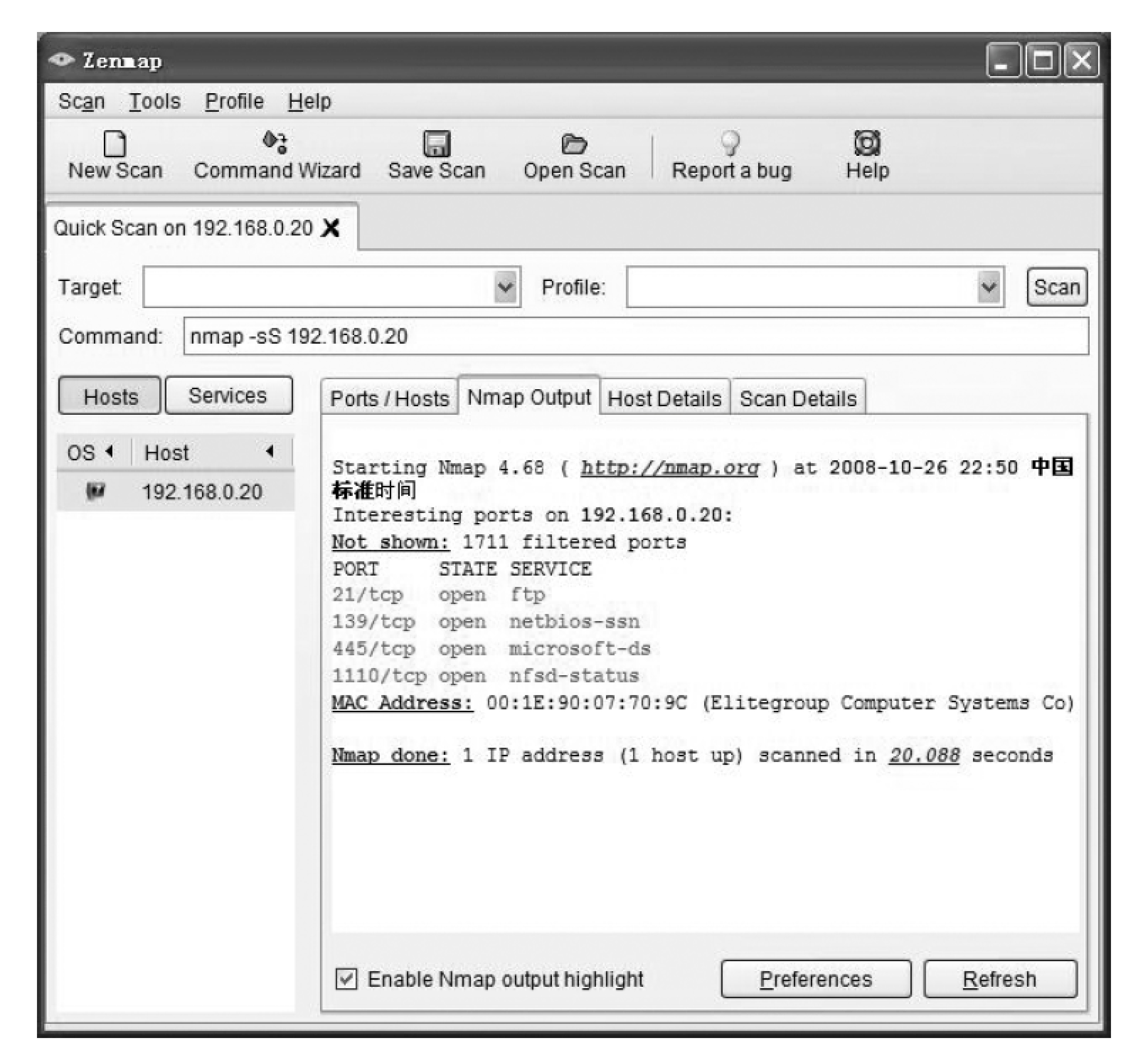


图 6-7　探测到目标主机上四个开放端口

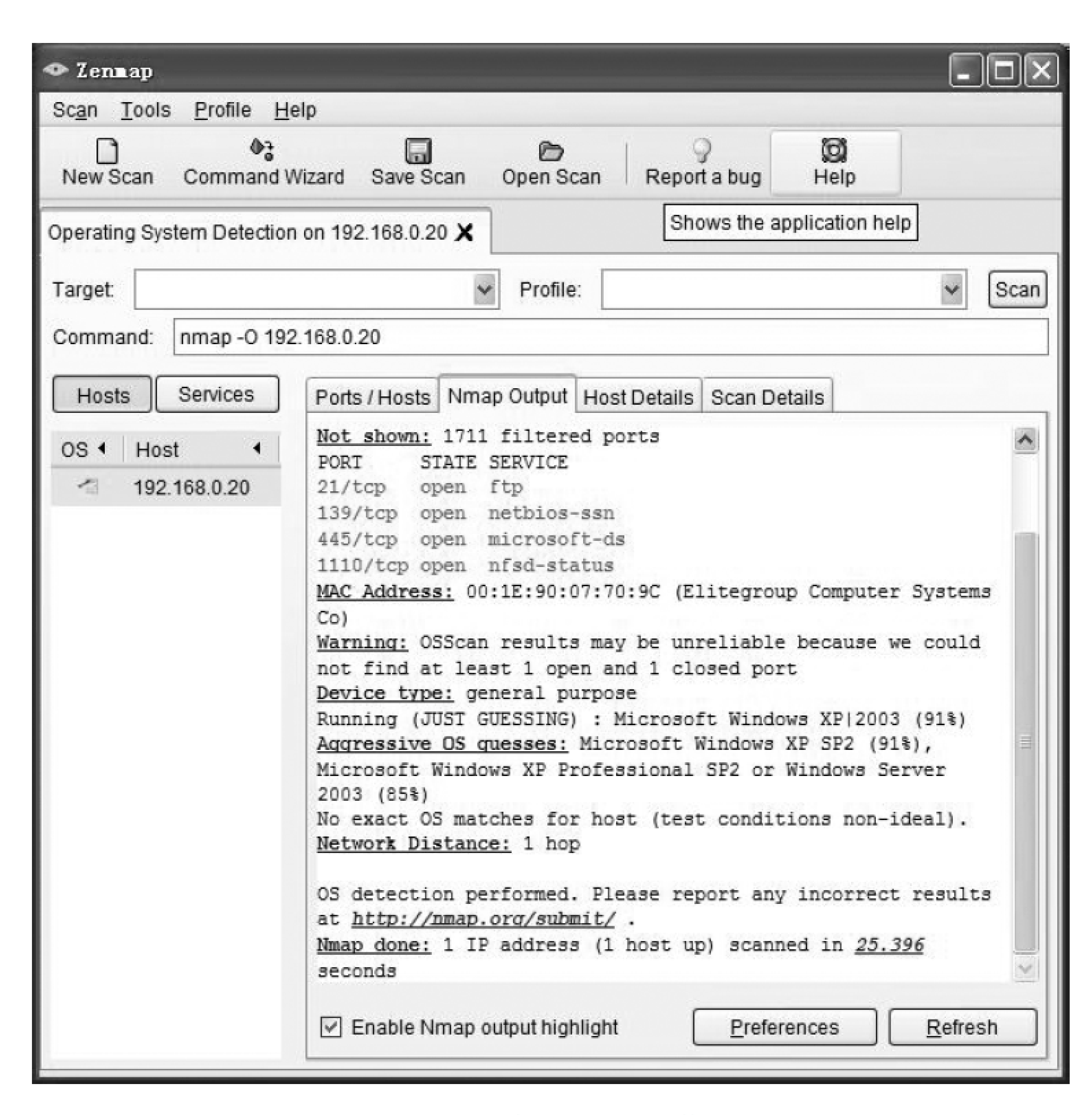


图 6-8　探测到目标主机的操作系统类型



2．检测入侵事件并查看相关内容

在目标主机(192.168.1.20)上可以检测到上述入侵事件(图 6-9),分别选择【统计信息】(图 6-10)、【会话】、【日志】选项,可以查看相关内容。



图 6-9　查看入侵事件



图 6-10　查看统计信息

3．导出记录

检测结果可以通过【文件】/【导出】命令,保存为三种类型的文件(图 6-11)。单击【下一



步】按钮，选择需要导出的记录项目，单击【完成】按钮，即可完成记录的导出。



图 6-11 【选择文件类型】对话框

4. 入侵规则设置

选择【设置】/【入侵规则设置】命令可以对各种入侵行为进行规则定义或编辑(图 6-12)，便于系统检测到各种入侵行为时做出不同的反应。



图 6-12 【入侵规则设置】对话框



6.5　Snort 入侵检测系统

6.5.1　Snort 介绍

1. Snort 概述

Snort 是一款免费、开源的网络入侵检测系统(Network Intrusion Detection System, NIDS),具有小巧灵便、易于配置、检测效率高等特性,常被称为轻量级的 IDS。Snort 具有实时数据流量分析和 IP 数据包日志分析能力,具有跨平台特征,能够进行协议分析和对内容的搜索或匹配。Snort 能够检测不同的攻击行为,如缓冲区溢出、端口扫描和拒绝服务攻击等,并进行实时报警。Snort 遵循通用公共许可证 GPL,只要遵守 GPL 的任何组织和个人都可以自由使用。

Snort 可以根据用户事先定义的一些规则分析网络数据流,并根据检测结果采取一定的行动。Snort 有 3 种工作模式,即嗅探器、数据包记录器和 NIDS。嗅探器模式仅从网络上读取数据包并作为连续不断的数据流显示在终端上;数据包记录器模式把数据包记录到硬盘上,以备分析之用;NIDS 模式功能强大,可以通过配置实现。

2. Snort 体系结构

Snort 的结构由以下四大软件模块组成。

(1) 数据包嗅探模块。数据包嗅探模块是一个并联在网络中的设备(可以是硬件,也可以是软件),它的工作原理和电话窃听很相似,不同的只是电话窃听的是语音网络,而数据包嗅探的是数据网。数据包嗅探模块主要功能为:网络分析和网络故障查找;网络性能和负荷量分析;监听明文传输的用户名密码等敏感数据。作为嗅探器,Snort 能够把捕获的数据包保存起来并可在事后查看。

(2) 预处理模块。预处理模块用相应的插件(例如 RPC 插件和端口扫描插件)检查原始数据包,从中发现这些数据的“行为”——原始数据包的应用层表现是什么。数据包经过预处理后才传到检测引擎。

(3) 检测引擎模块。检测引擎模块是 Snort 的核心模块。当数据包从预处理器送过来后,检测引擎依据预先设置的规则检查数据包,一旦发现数据包中的内容和某条规则相匹配,就通知报警模块。

(4) 报警/日志模块。经检测引擎检查后的 Snort 数据需要以某种方式输出。如果检测引擎中的某条规则被匹配,则会触发一条报警,这条报警信息会通过网络、UNIXSocket、Windows Popup(SMB)、SNMP 协议的 Trap 命令传送给日志文件,甚至可以将报警传送给第三方插件(如 SnortSam)。另外,报警信息也可以记入 SQL 数据库,如 MySQL 或 Postgres 等。

Snort 体系结构如图 6-13 所示。



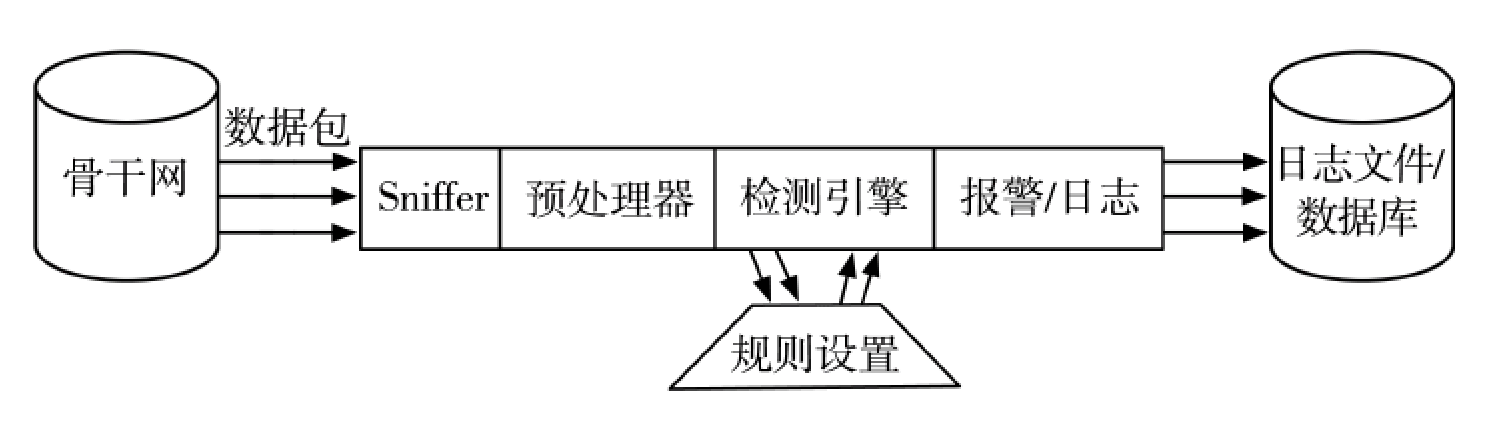


图 6-13　Snort 体系结构

6.5.2　部署 Snort 入侵检测系统

部署 Snort 入侵检测系统所需软件如下。

(1) Apache(Windows 版本的 apache Web 服务器)

下载地址：http://www.apache.org

(2) Acid(基于 PHP 的入侵检测数据库分析控制台)

下载地址：http://www.cert.org/kb/acid

(3) Adodb(Adodb(Active Data Objects Data Base)库 for PHP)

下载地址：http://jaist.dl.sourceforge.net/sourceforge/adodb/adodb504.tgz

(4) JPGraph(PHP 下面的图形库)

下载地址：http://www.aditus.nu/jpgraph

(5) MySQL(Windows 版本的 MySQL 数据库服务器)

下载地址：http://www.mysql.com/

(6) PHP(Windows 版本的 PHP 脚本环境支持)

下载地址：http://www.php.net/

(7) Snort(在 Windows 平台下的 snort 安装包,Linux 平台的到官网下载)

下载地址：http://www.snort.org/

(8) Winpcap(Windows 版本的 PCAP,网络数据包截取驱动程序)

下载地址：http://winpcap.polito.it/

(9) Snortrules(Snort 检测规则库)

到官方网站下载,需要注册用户。

也有不需注册的版本,下载地址：http://www.snort.org/pub-bin/downloads.cgi

官方下载地址：http://www.snort.org/pub-bin/downloads.cgi/Download/vrt_pr/snortrules-pr-2.4.tar.gz

(10) php5apache2.dll-php5.1.x.zip(用于在 Apache 下正常显示的 PHP 补丁)

下载地址：http://www.php.net

部署并使用 Snort 入侵检测系统需要经过如图 6-14 所示步骤。

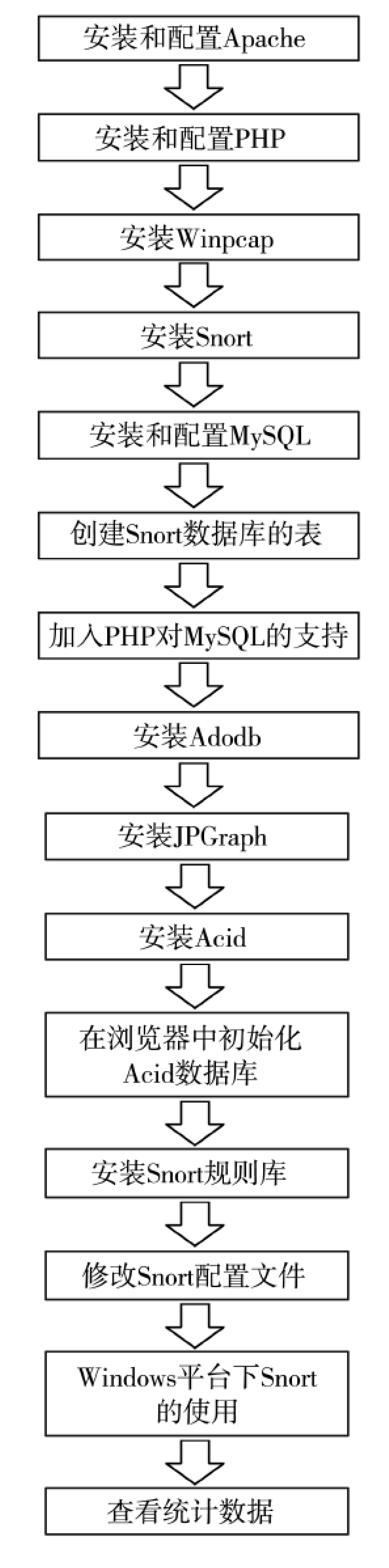


图 6-14　部署 Snort 入侵检测系统步骤



Snort 入侵检测系统建议部署在 Windows Server 2003 的计算机中。详细操作步骤如下。

1. 安装和配置 Apache

(1) 按默认选项进行安装。当出现 Server Information(服务器信息)对话框时,填入相关信息,如图 6-15 所示。然后依次按提示单击 Next 按钮,当出现 Destination Folder(目标文件夹)页面时,可单击 Change(改变)按钮,设定安装路径,如图 6-16 所示。其余按默认选项安装即可。安装过程可能会出现如图 6-17 所示页面,按 Esc 键跳过即可。

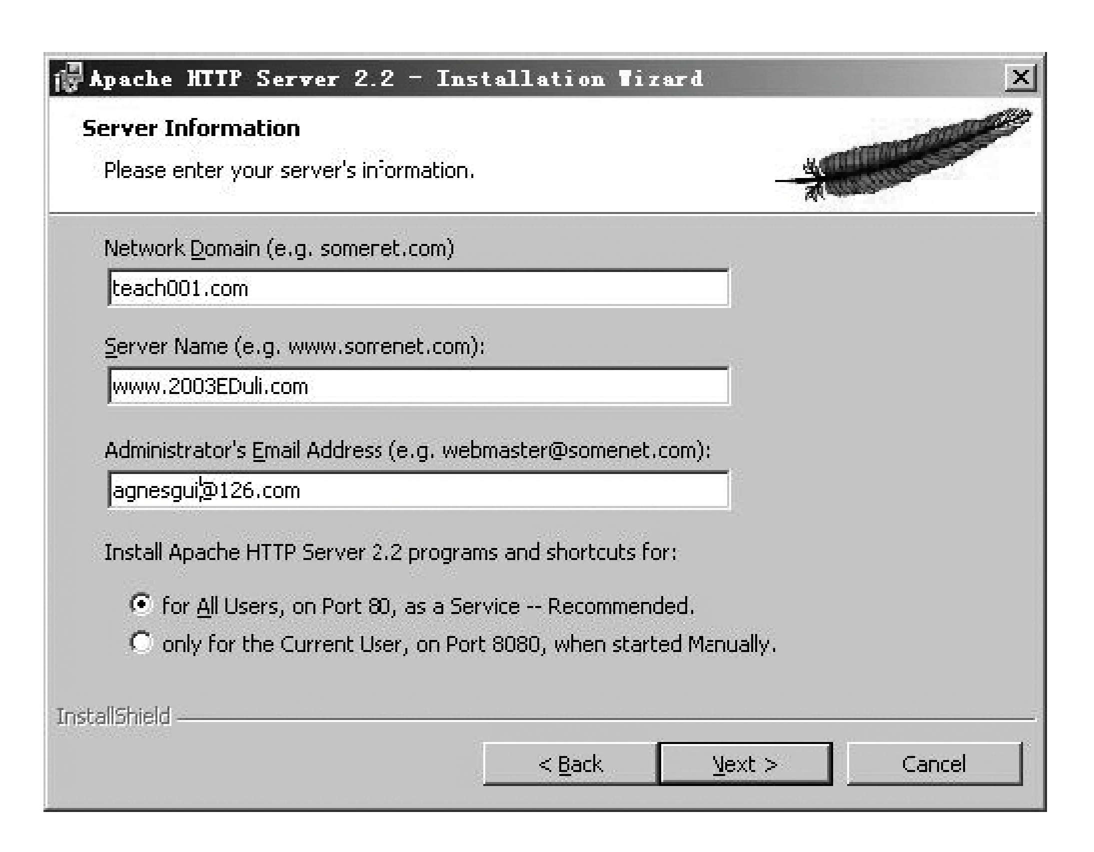



图 6-15 Server Information 对话框



图 6-16 Destination Folder 页面



图 6-17 提示页面

(2) 修改 C:\Apache2.2\conf 文件夹中的 httpd.conf 文件,如图 6-18 所示,将监听端口 80 改为 8008。

(3) 重新启动计算机,在 IE 浏览器的地址栏输入:http://localhost:8008/,如果出现如图 6-19 所示界面,则说明 Apache 软件安装成功了。



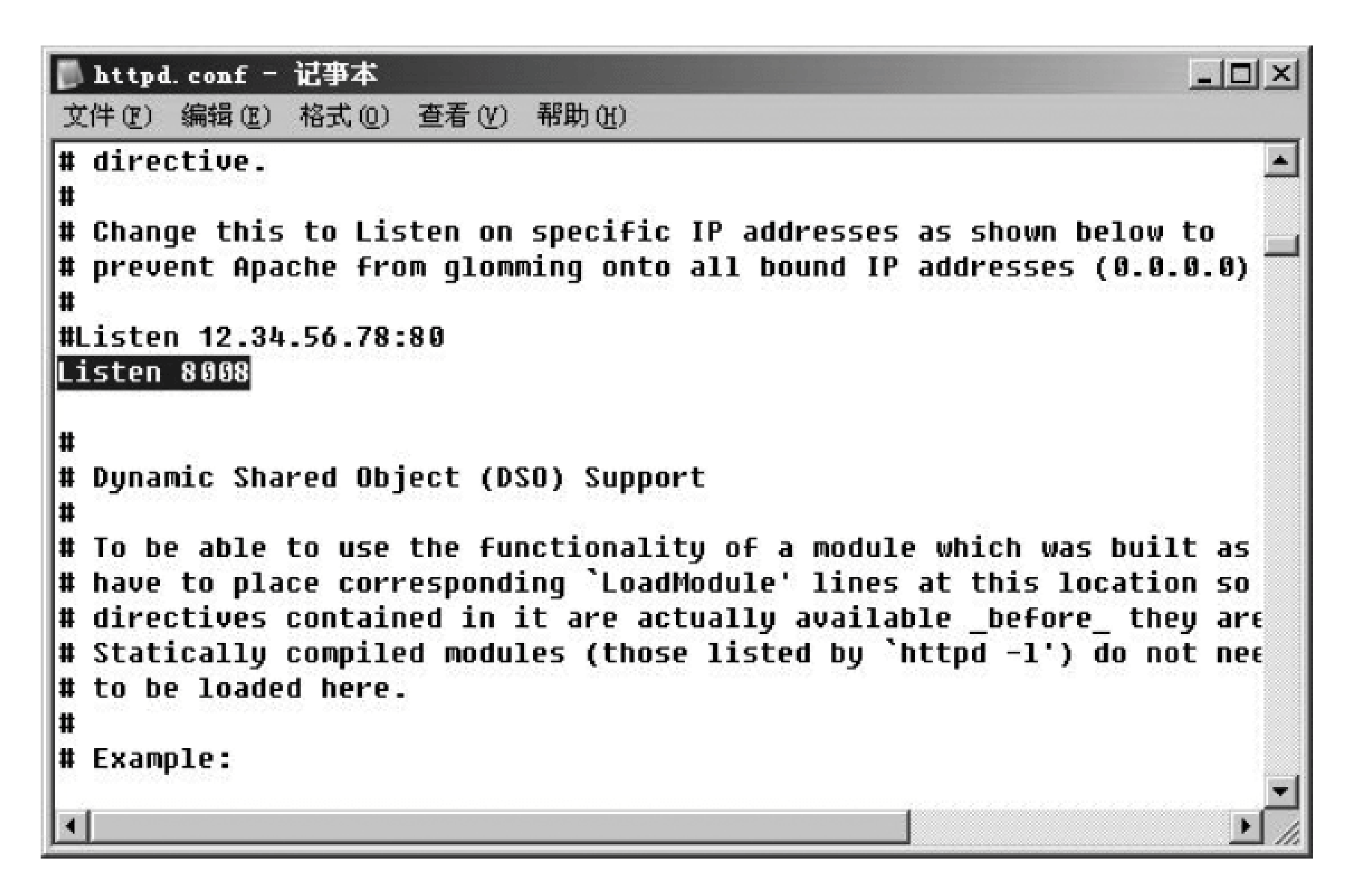


图 6-18 httpd.conf 文件内容

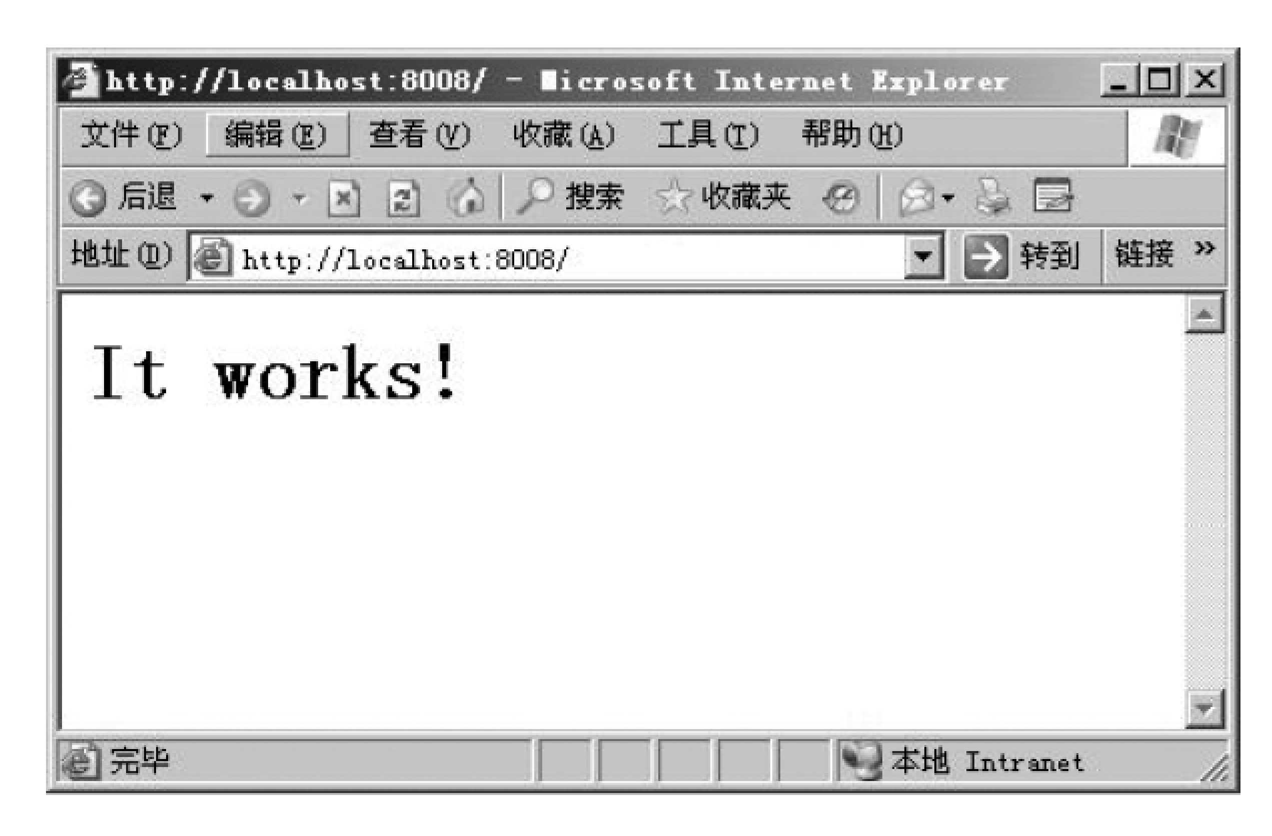


图 6-19 http://localhost 页面

2. 安装和配置 PHP

(1) 解压缩 php-5.1.6-Win32.zip 到 C:\php 文件夹。

(2) 将 C:\php 文件夹中的 php5ts.dll 文件复制到 C:\Windows\system32 文件夹，将 php.ini-dist 文件复制到 C:\Windows，并重命名为 php.ini。

(3) 修改 C:\Apache2.2\conf 文件夹中的 httpd.conf 文件，在图 6-20 处添加如下语句：Loadmodule php5_module C: \php\php5apache2.dll。

在如图 6-21 处添加如下语句：Addtype application/x-httpd-php .php(注意空格)。

(4) 安装 PHP 补丁 php5apache2.dll-php5.1.x.zip

① 解压缩 php5apache2.dll-php5.1.x.zip 到 C:\ php5apache2.dll-php5.1.x 文件夹。

② 将 php5apache2.dll-php5.1.x 文件夹中 httpd.exe.manifest 文件复制到 C:\Apache2.2\bin 文件夹。

③ 将 php5apache2.dll-php5.1.x 文件夹中 php5apache2.dll 文件复制到 C:\php 文件夹，覆盖原文件。

④ 双击 php5apache2.dll-php5.1.x 文件夹中 vcredist_x86.exe 文件进行安装。



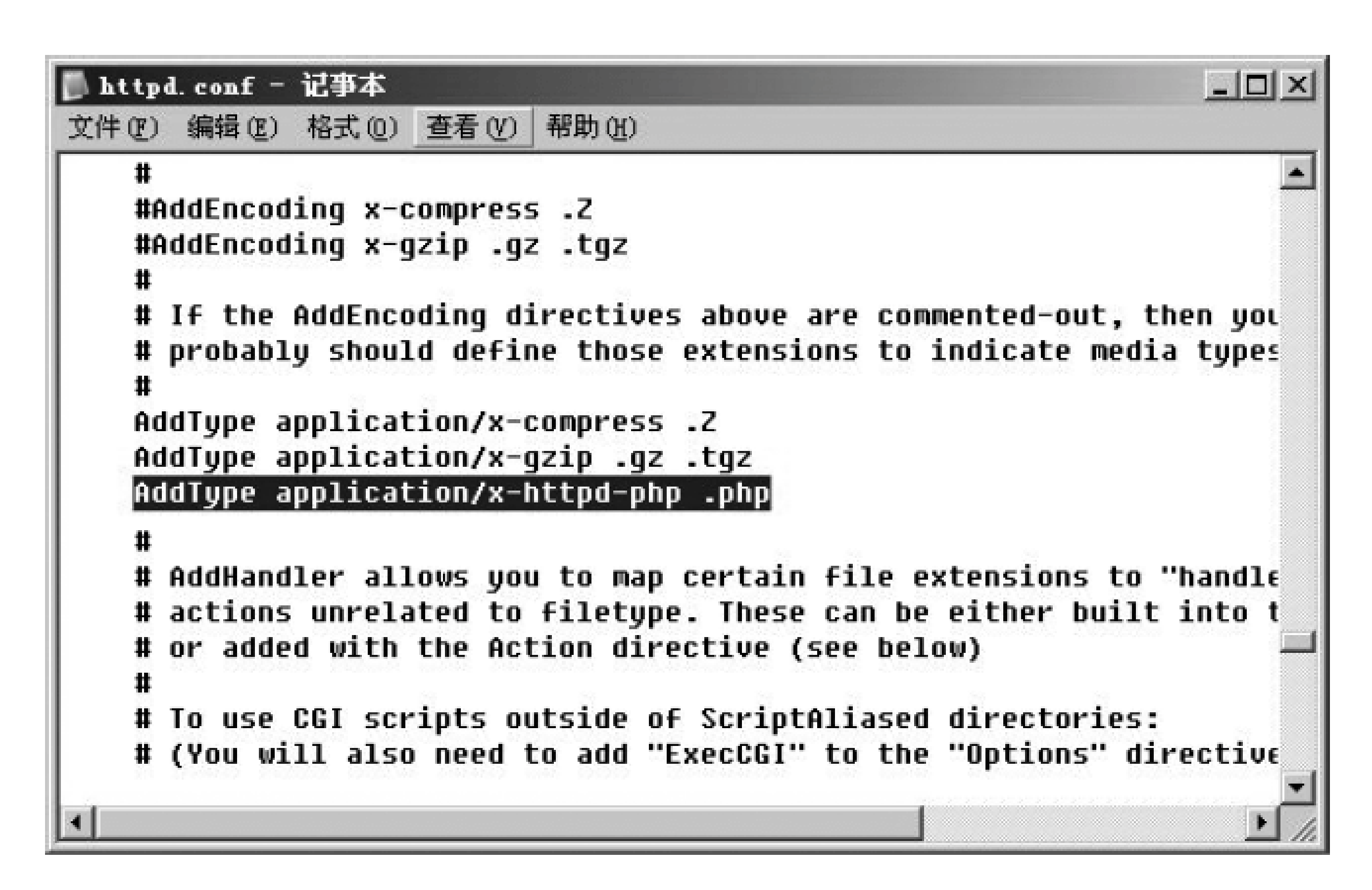




```
httpd.conf - 记事本
文件(F)  编辑(E)  格式(O)  查看(V)  帮助(H)
#LoadModule proxy_connect_module modules/mod_proxy_connect.so
#LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule negotiation_module modules/mod_negotiation.so
#LoadModule rewrite_module modules/mod_rewrite.so
LoadModule setenvif_module modules/mod_setenvif.so
#LoadModule speling_module modules/mod_speling.so
#LoadModule status_module modules/mod_status.so
#LoadModule unique_id_module modules/mod_unique_id.so
LoadModule userdir_module modules/mod_userdir.so
#LoadModule usertrack_module modules/mod_usertrack.so
#LoadModule vhost_alias_module modules/mod_vhost_alias.so
#LoadModule ssl_module modules/mod_ssl.so
LoadModule php5_module C:/php/php5apache2.dll

# 'Main' server configuration
#
# The directives in this section set up the values used by the 'main'
```

图 6-20　httpd. conf 文件内容(一)



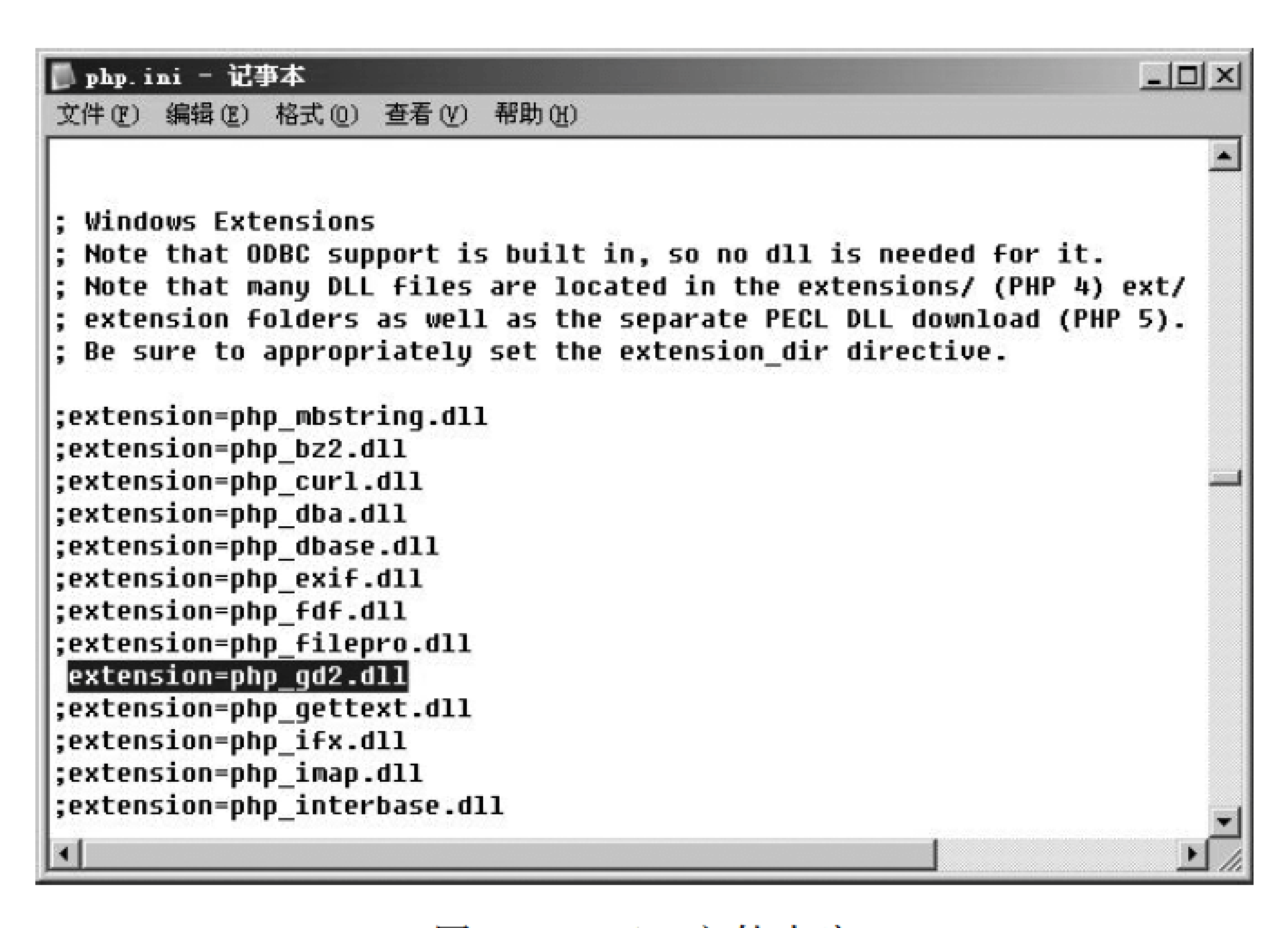
```
httpd.conf - 记事本
文件(F)  编辑(E)  格式(O)  查看(V)  帮助(H)
    #
    #AddEncoding x-compress .Z
    #AddEncoding x-gzip .gz .tgz
    #
    # If the AddEncoding directives above are commented-out, then you
    # probably should define those extensions to indicate media types
    #
    AddType application/x-compress .Z
    AddType application/x-gzip .gz .tgz
    AddType application/x-httpd-php .php

    #
    # AddHandler allows you to map certain file extensions to "handle
    # actions unrelated to filetype. These can be either built into t
    # or added with the Action directive (see below)
    #
    # To use CGI scripts outside of ScriptAliased directories:
    # (You will also need to add "ExecCGI" to the "Options" directive
```

图 6-21　httpd. conf 文件内容(二)

(5) 添加 apache 对 GD 库的支持

① 修改 C:\Windows 文件夹中的 php. ini 文件，删除 extension＝php_gd2. dll 语句前的分号(图 6-22)。



```
php.ini - 记事本
文件(F)  编辑(E)  格式(O)  查看(V)  帮助(H)

; Windows Extensions
; Note that ODBC support is built in, so no dll is needed for it.
; Note that many DLL files are located in the extensions/ (PHP 4) ext/
; extension folders as well as the separate PECL DLL download (PHP 5).
; Be sure to appropriately set the extension_dir directive.

;extension=php_mbstring.dll
;extension=php_bz2.dll
;extension=php_curl.dll
;extension=php_dba.dll
;extension=php_dbase.dll
;extension=php_exif.dll
;extension=php_fdf.dll
;extension=php_filepro.dll
 extension=php_gd2.dll
;extension=php_gettext.dll
;extension=php_ifx.dll
;extension=php_imap.dll
;extension=php_interbase.dll
```

图 6-22　php 文件内容



② 将 C:\php\ext 文件夹中的 php_gd2.dll 文件复制到 C:\Windows 文件夹。

(6) 测试 PHP 安装是否成功

① 在 C:\apache\htdocs 文件夹中新建 test.php 文件，用记事本打开，编辑内容为 <? phpinfo () ;? >。

② 重新启动 Apache 服务(先选择 Stop 选项，再选择 Start 选项)，如图 6-23 和图 6-24 所示。



图 6-23　选择 Stop 选项



图 6-24　选择 Start 选项

③ 在 IE 浏览器的地址栏输入：http://lcoalhost:8008/test.php 测试是否安装成功，成功的界面如图 6-25 所示。

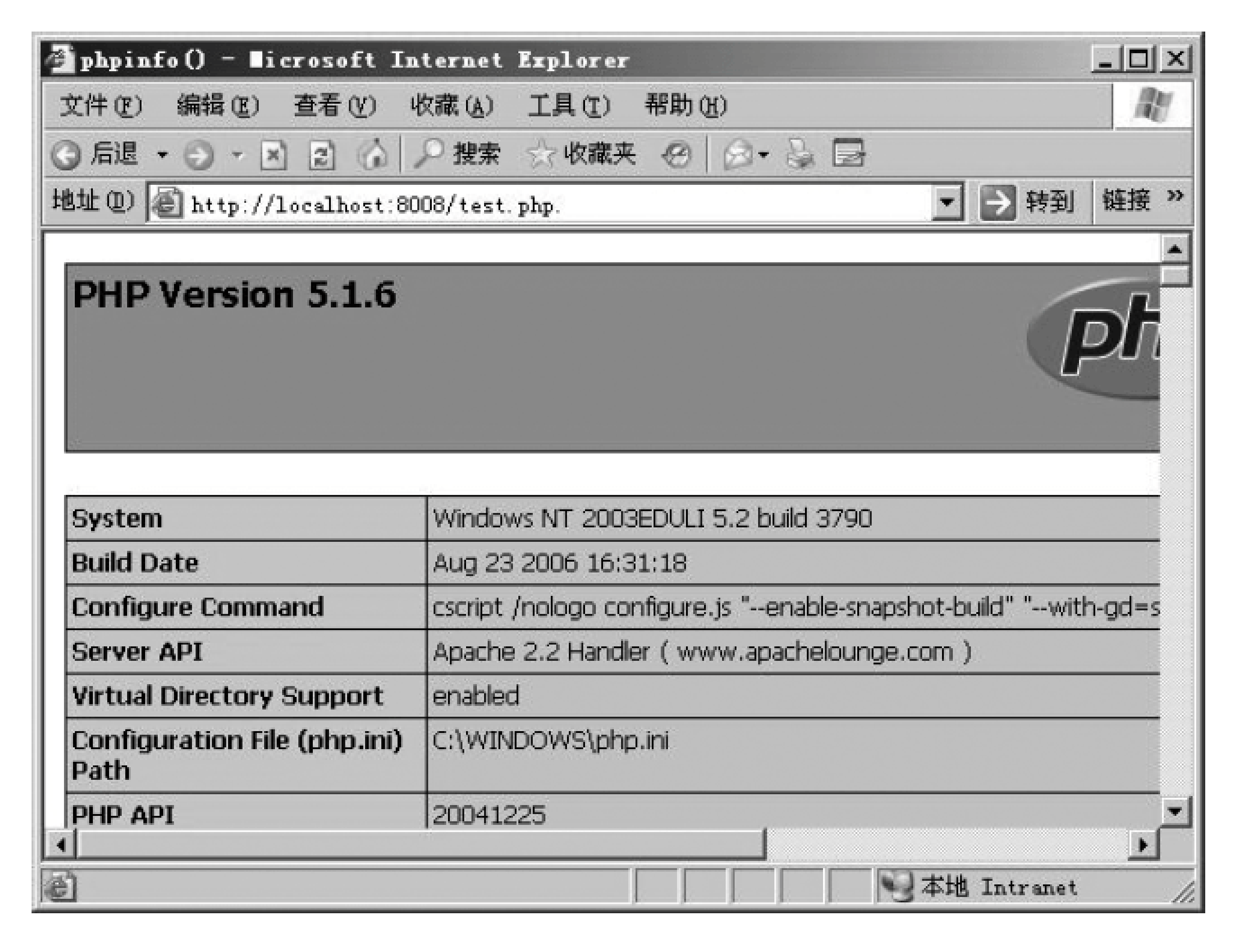


图 6-25　http://lcoalhost:8008/test.php 测试页面

3. 安装 Winpcap

采取默认值即可。

4. 安装 Snort

指定路径为 C:\Snort，其余情况采取默认值即可。

在命令行方式下输入如下命令：

```
C:\Snort\bin>snort-W
```

如果安装成功，系统将显示出如图 6-26 所示信息。



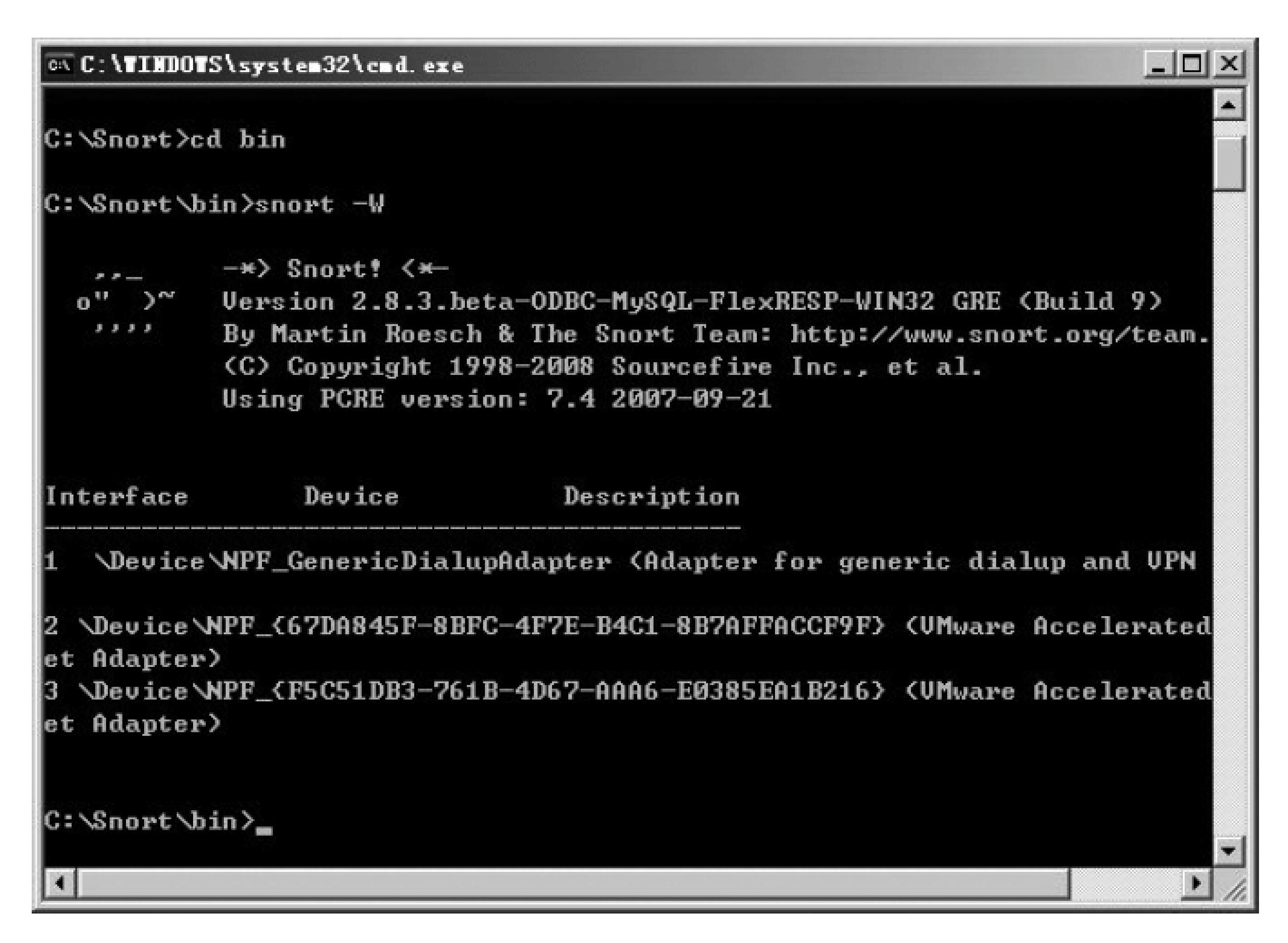


图 6-26　snort-W 页面

5．安装和配置 MySQL

在不特别注明的情况下，按默认选项安装。

(1) 当安装进行到出现 Setup Type(安装类型)对话框时，选择 Custom(习惯)单选按钮，单击 Next 按钮。

(2) 指定安装路径为 C:\MySQL。

(3) 当安装进行到出现 MySQL Server Instance Configuration(MySQL 服务器实例配置)的 Please select a configuration type(请选择一个配置类型)对话框时，选择 Standard Configuration(标准配置)单选按钮，单击 Next 按钮。

(4) 当安装进行到出现 MySQL Server Instance Configuration 的 Please set the security options(请设置安全选项)对话框时，请设置登录密码(图 6-27)，单击 Next 按钮。

(5) 当安装进行到出现 MySQL Server Instance Configuration 的 Ready to execute...(准备执行)对话框时，单击 Execute 按钮执行(图 6-28)。最后单击 Finish 按钮完成安装。



图 6-27　Please set the security options 对话框

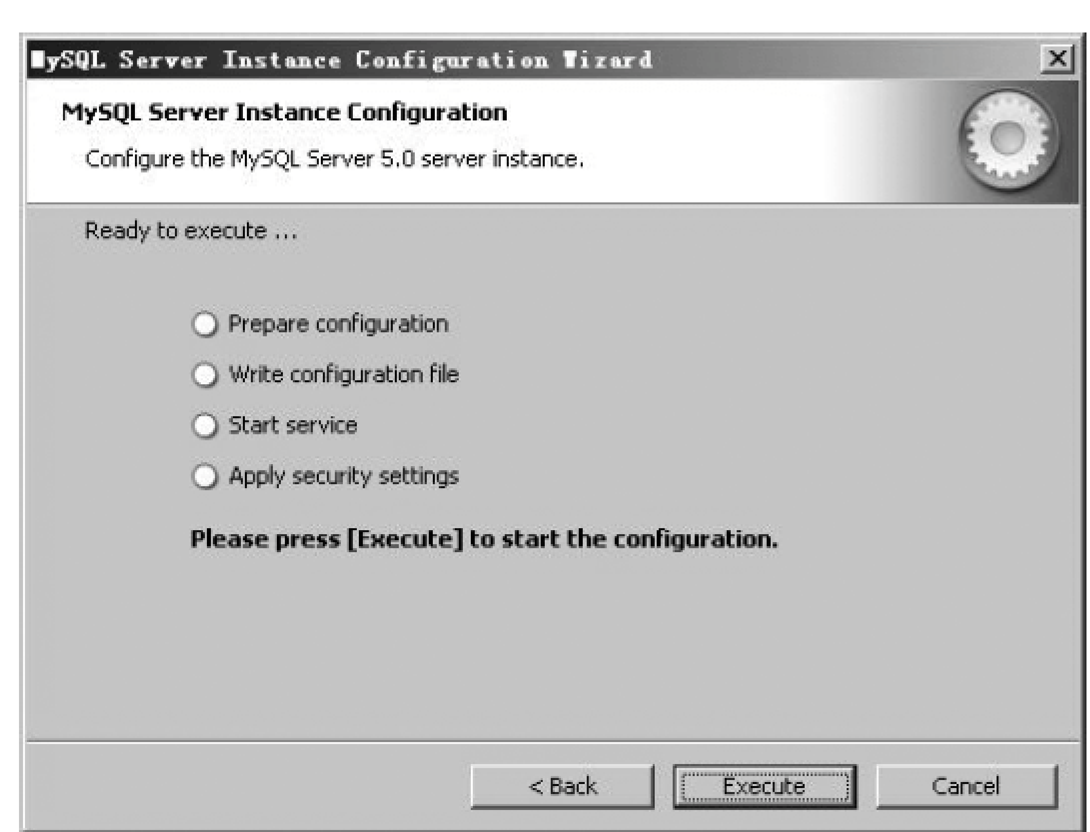


图 6-28　Ready to execute...对话框



6. 创建 Snort 数据库的表

将 C:\Snort\schames 文件夹中的 create_mysql 文件复制到 C:\MySQL\bin 文件夹。

执行 MySQL 客户端(图 6-29),在打开的 MySQL Command Line Client(MySQL 的命令行客户端)对话框中输入密码,并依次执行如下命令(图 6-30)。

```
mysql>Create database snort;
mysql>Create database snort_archive;
mysql>Use snort;
mysql>Source create_mysql;
mysql>Use snort_archive;
mysql>Source create_mysql;
mysql>Grant all on* .* to"root"@"localhost";
```

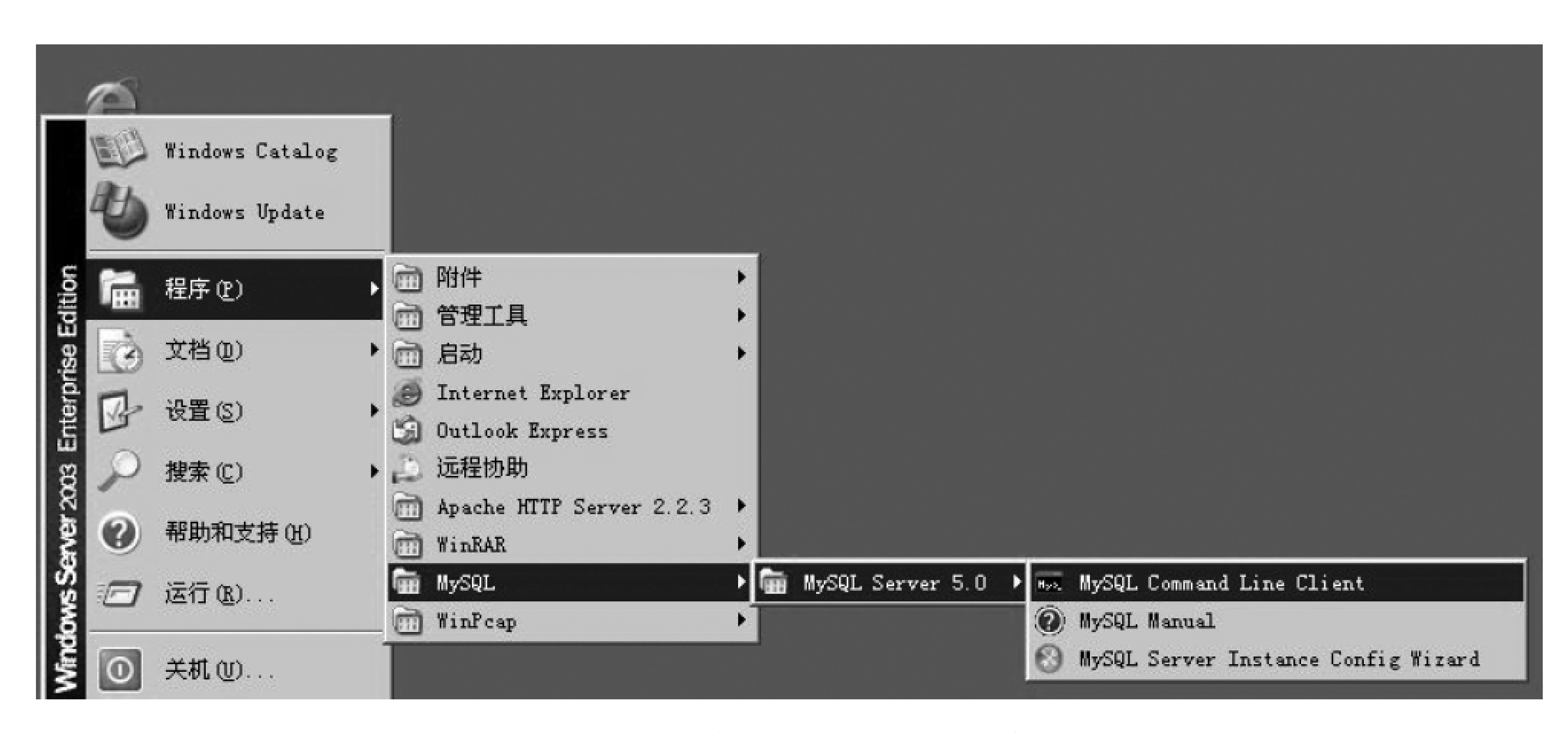


图 6-29 执行 MySQL 客户端

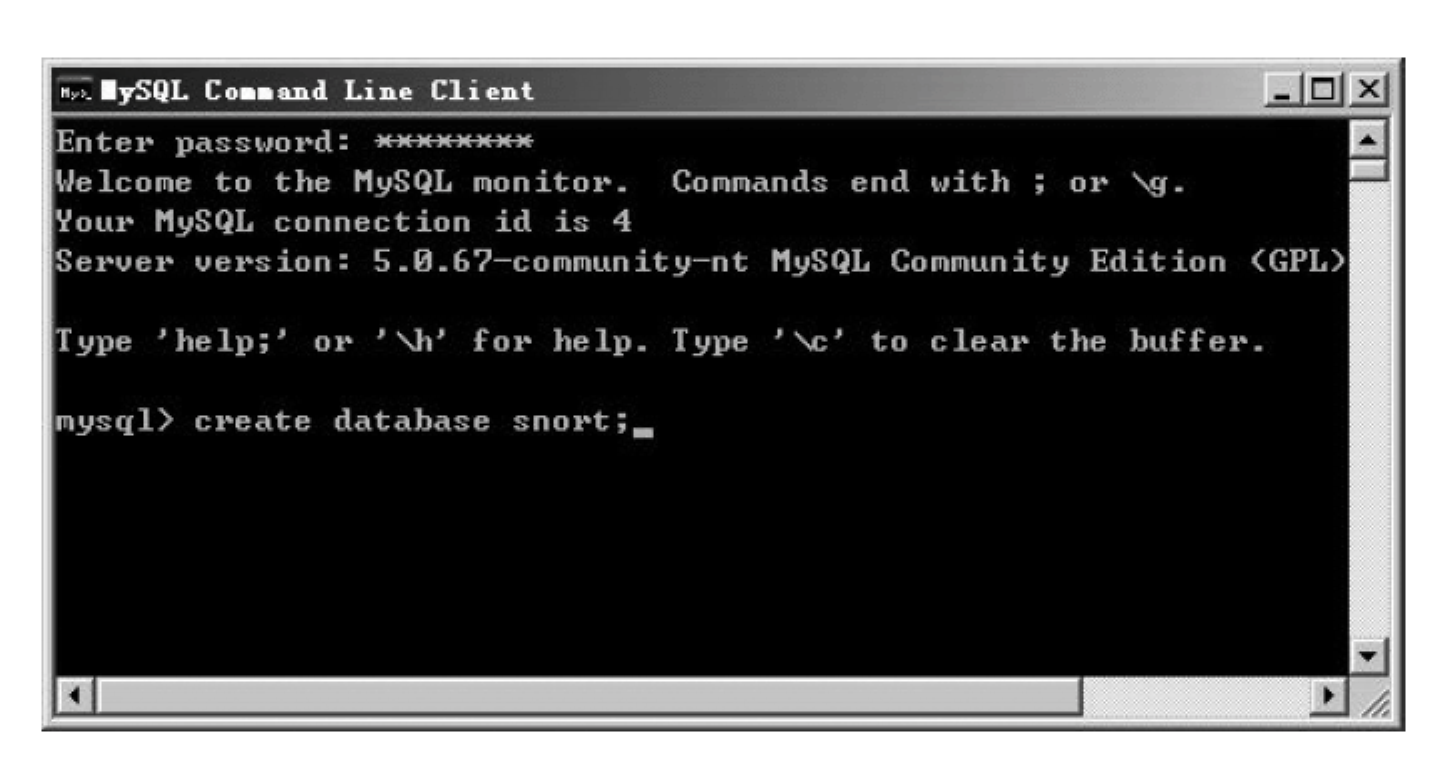


图 6-30 MySQL Command Line Client 对话框

7. 加入 PHP 对 MySQL 的支持

(1) 修改 C:\Windows\php.ini 文件,去掉 extension=php_mysql.dll 前的分号(图 6-31)。

(2) 将 C:\php\ext 文件夹下的 php_mysql.dll 文件复制到 C:\Windows 文件夹。





php.ini - 记事本

文件(F)　编辑(E)　格式(O)　查看(V)　帮助(H)

```
;extension=php_imap.dll
;extension=php_interbase.dll
;extension=php_ldap.dll
;extension=php_mcrypt.dll
;extension=php_mhash.dll
;extension=php_mime_magic.dll
;extension=php_ming.dll
;extension=php_mssql.dll
;extension=php_msql.dll
extension=php_mysql.dll
;extension=php_oci8.dll
;extension=php_openssl.dll
;extension=php_oracle.dll
```

图 6-31　php.ini 内容

（3）将 C:\php 文件夹下的 libmysql.dll 文件复制到 C:\Windows\system32 下。

8．安装 Adodb

解压缩 Adodb 到 C:\php\adodb 文件夹。

9．安装 JPGraph

解压缩 JPGraph 到 C:\php\jpgraph 文件夹。

10．安装 Acid

（1）解压缩 Acid 到 C:\apache2.2\htdocs\acid 文件夹。修改 acid 文件夹中的 acid_conf.php 文件的以下语句为正确的路径(图 6-32 和图 6-33)。

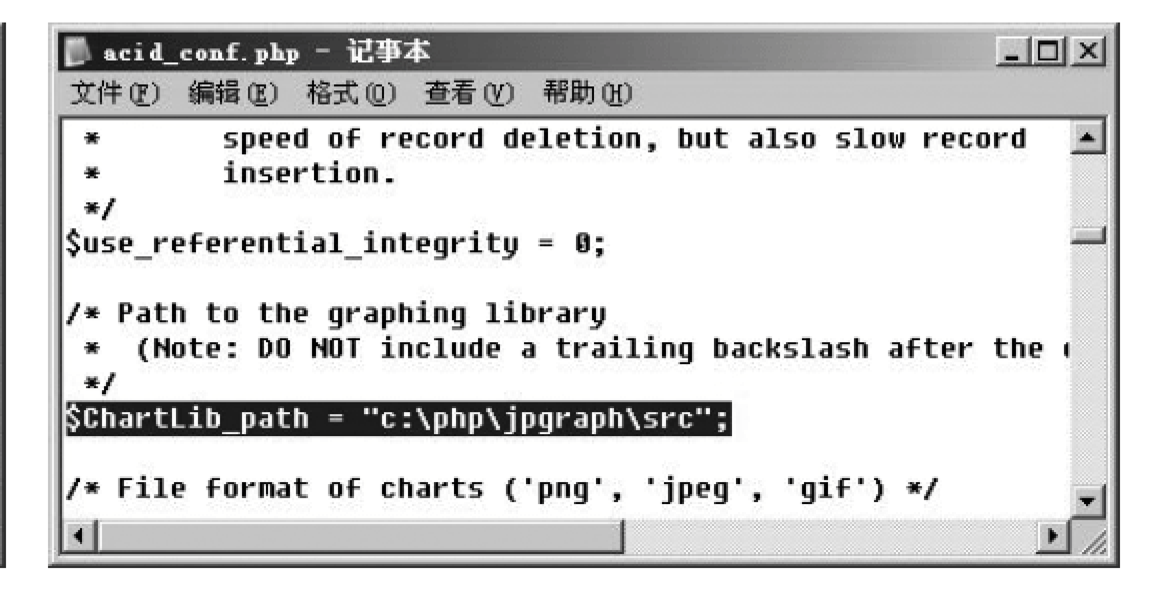
acid_conf.php - 记事本

文件(F)　编辑(E)　格式(O)　查看(V)　帮助(H)

```
 *   e.g. $foo = "/tmp"      [OK]
 *        $foo = "/tmp/"     [OK]
 *        $foo = "c:\tmp"    [OK]
 *        $foo = "c:\tmp\"   [WRONG]
 */
$DBlib_path = "c:\php\adodb";

/* The type of underlying alert database
 *
 *  MySQL       : "mysql"
 *  PostgresSQL : "postgres"
```

图 6-32　acid_conf.php 内容(一)



acid_conf.php - 记事本

文件(F)　编辑(E)　格式(O)　查看(V)　帮助(H)

```
 *        speed of record deletion, but also slow record
 *        insertion.
 */
$use_referential_integrity = 0;

/* Path to the graphing library
 *  (Note: DO NOT include a trailing backslash after the 
 */
$ChartLib_path = "c:\php\jpgraph\src";

/* File format of charts ('png', 'jpeg', 'gif') */
```

图 6-33　acid_conf.php 内容(二)

```
$DBlib_path="c:\php\adodb";
$ChartLib_path="c:\php\jpgraph\src";
```

（2）确保 acid_conf.php 相关语句为下列的值。

```
$alert_dbname      ="snort";
$alert_host        ="localhost";
$alert_port        ="3306";
$alert_user        ="root";
```



```
$ alert_password    ="123456";
$ archive_dbname    ="snort_archive";
$ archive_host      ="localhost";
$ archive_port      ="3306";
$ archive_user      ="root";
$ archive_password ="123456";
```

(3) 重新启动 Apache 和 MySQL 服务。

11. 在浏览器中初始化 Acid 数据库

在 IE 浏览器的地址栏输入：http://localhost:8008/acid/acid_db_setup.php，如果配置正确，会出现如图 6-34 所示页面。单击 Create ACID AG 按钮，让系统自动在 MySQL 中建立 Acid 运行必须的数据库，出现如图 6-35 所示页面则表示成功。

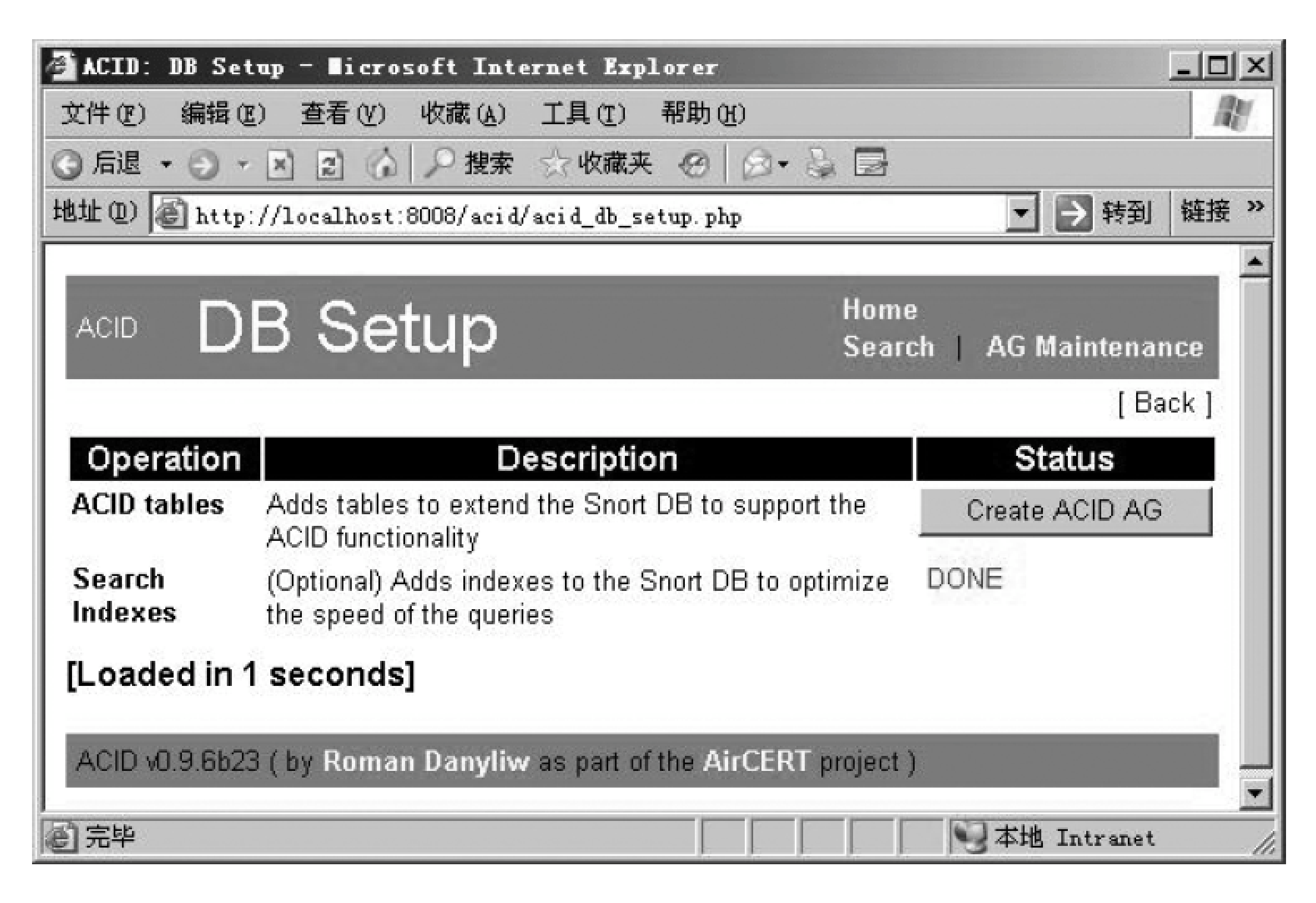


图 6-34　ACID DB Setup 页面

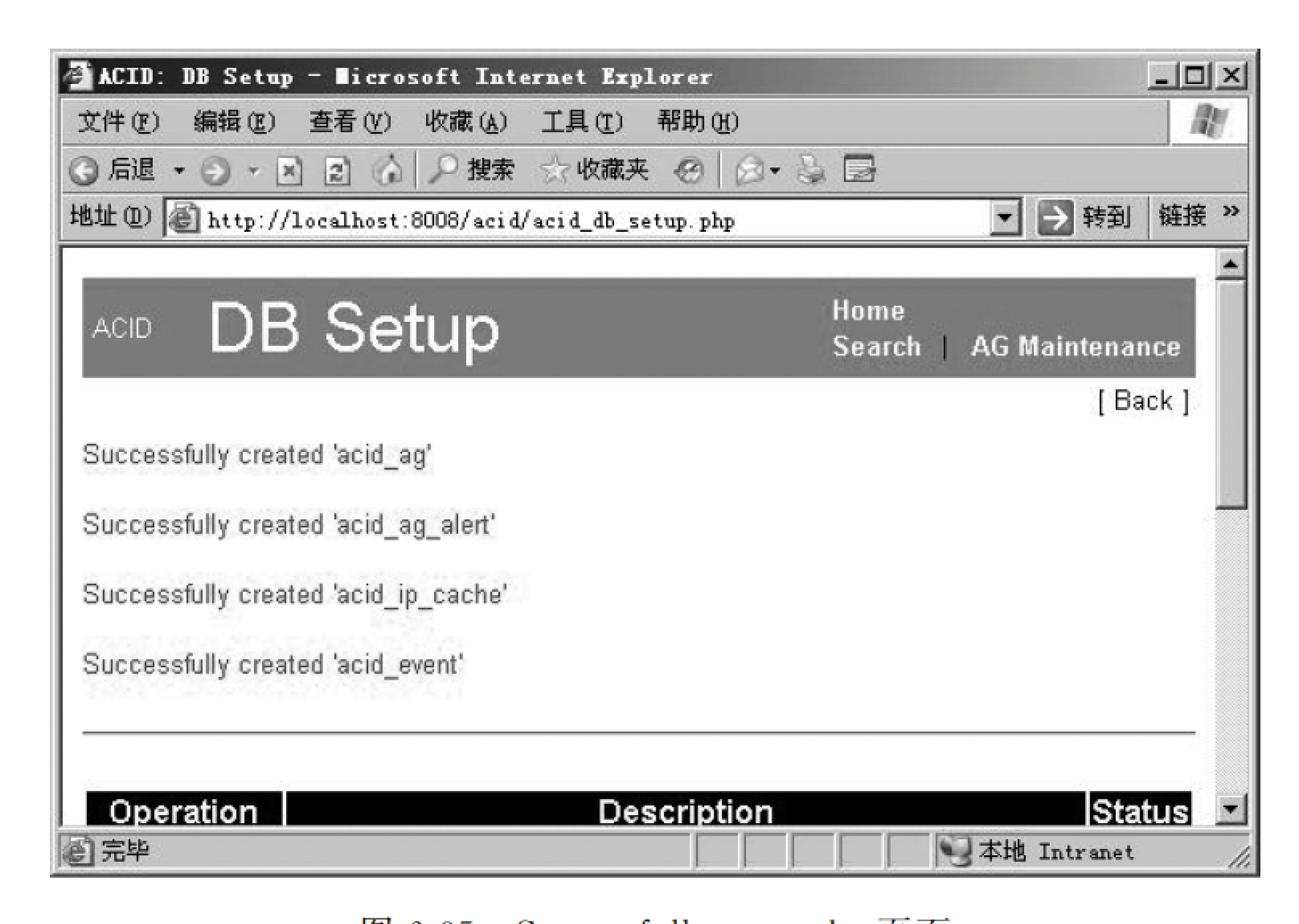


图 6-35　Successfully created...页面





12. 安装 Snort 规则库

解压缩 rules 到 C:\Snort\rules 文件夹。

13. 修改 Snort 配置文件

用写字板打开 C:\Snort\etc 文件夹中的 snort.conf 文件。

(1) 设置 Snort 的内部网络和外部网络检测范围。将 snort.conf 文件中的 var HOME_NET any 语句中的 any 改为自己所在的子网地址,即将 Snort 监测的内部网络设置为本机所在的局域网。如本地 IP 为 192.168.3.23,则将 any 改为 192.168.3.0/24(图 6-36)。



图 6-36 snort.conf 配置文件内容(一)

(2) 配置网段内提供网络服务的 IP 地址,只需要把默认的 $ HOME NET 改成对应主机地址即可:

```
var DNS_SERVERS $ HOME NET
var SMTP_SERVERS $ HOME NET
var HTTP_SERVERS $ HOME NET
var SQL_SERVERS $ HOME NET
var TELNET_SERVERS $ HOME NET
var SNMP_SERVERS $ HOME NET
```

如果不需要监视某种类型的服务,可以用 # 号将上述语句注释掉。

注意: 由于该实验中提供上述网络服务的计算机就是本机,因此不用更改。

(3) 修改设置监测包含的规则。在配置文件末尾,定义了与规则相关的配置,格式如下:

```
include $ RULE PATH/local.rules
include $ RULE PATH/bad-traffic.rules
include $ RULE_PATH/exploit.rules
```

其中,变量 $RULE_PATH 指明了规则文件存放的路径,可以在语句 var RULEPATH .../rules 中将变量 RULE_PATH 改为存放规则集的目录,如 C:\Snort\rules。

(4) 修改配置文件 Classification.conf 和 Reference.conf 的路径:

```
Include C:\Snort\etc\classification.config
```



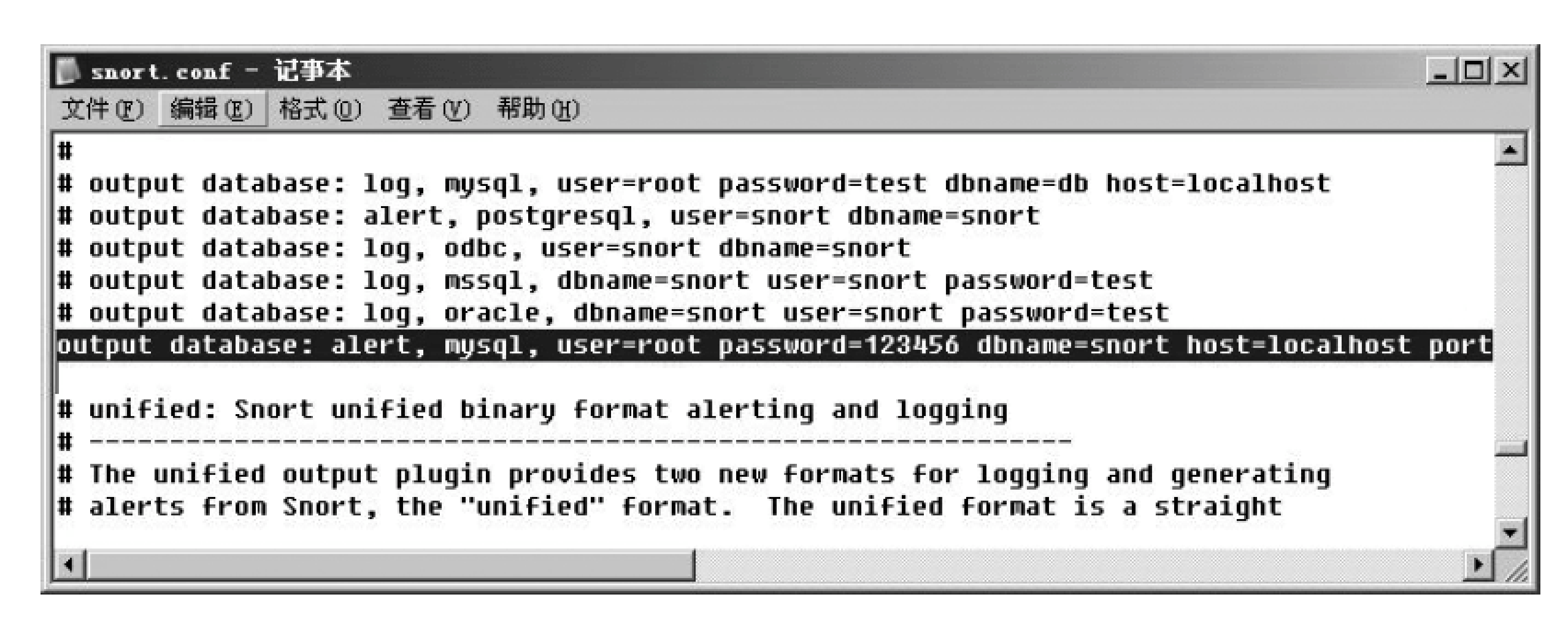
Include C:\Snort\etc\reference. config

其中,Classification. conf 文件保存的是和规则的警报级别相关的配置,Reference. conf 文件保存了提供更多警报相关信息的链接。

(5) 修改各文件路径如下。

dynamicengine/usr/local/lib/snort_dynamicengine/libsf_engine.so 改为:dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
dynamicpreprocessor directory/usr/local/lib/snort_dynamicpreprocessor/改为: dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor/
dynamicpreprocessor file< full path to libsf_dcerpc_preproc.so>改为:dynamicpreprocessor file C:\Snort\lib\snort_dynamicpreprocessor\sf_dcerpc.dll
dynamicpreprocessor file< full path to libsf_ftptelnet_preproc.so>改为:dynamicpreprocessor file C:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll
dynamicpreprocessor file< full path to libsf_dns_preproc.so>改为:dynamicpreprocessor file C:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll
dynamicpreprocessor file< full path to libsf_smtp_preproc.so>改为:dynamicpreprocessor file C:\Snort\lib\snort_dynamicpreprocessor\sf_smtp.dll
dynamicpreprocessor file< full path to libsf_ssh_preproc.so>改为:dynamicpreprocessor file C:\Snort\lib\snort_dynamicpreprocessor\sf_ssh.dll
include classification. config 改为:include C:\snort\etc\classification. config include reference.config 改为:include C:\snort\etc\reference.config

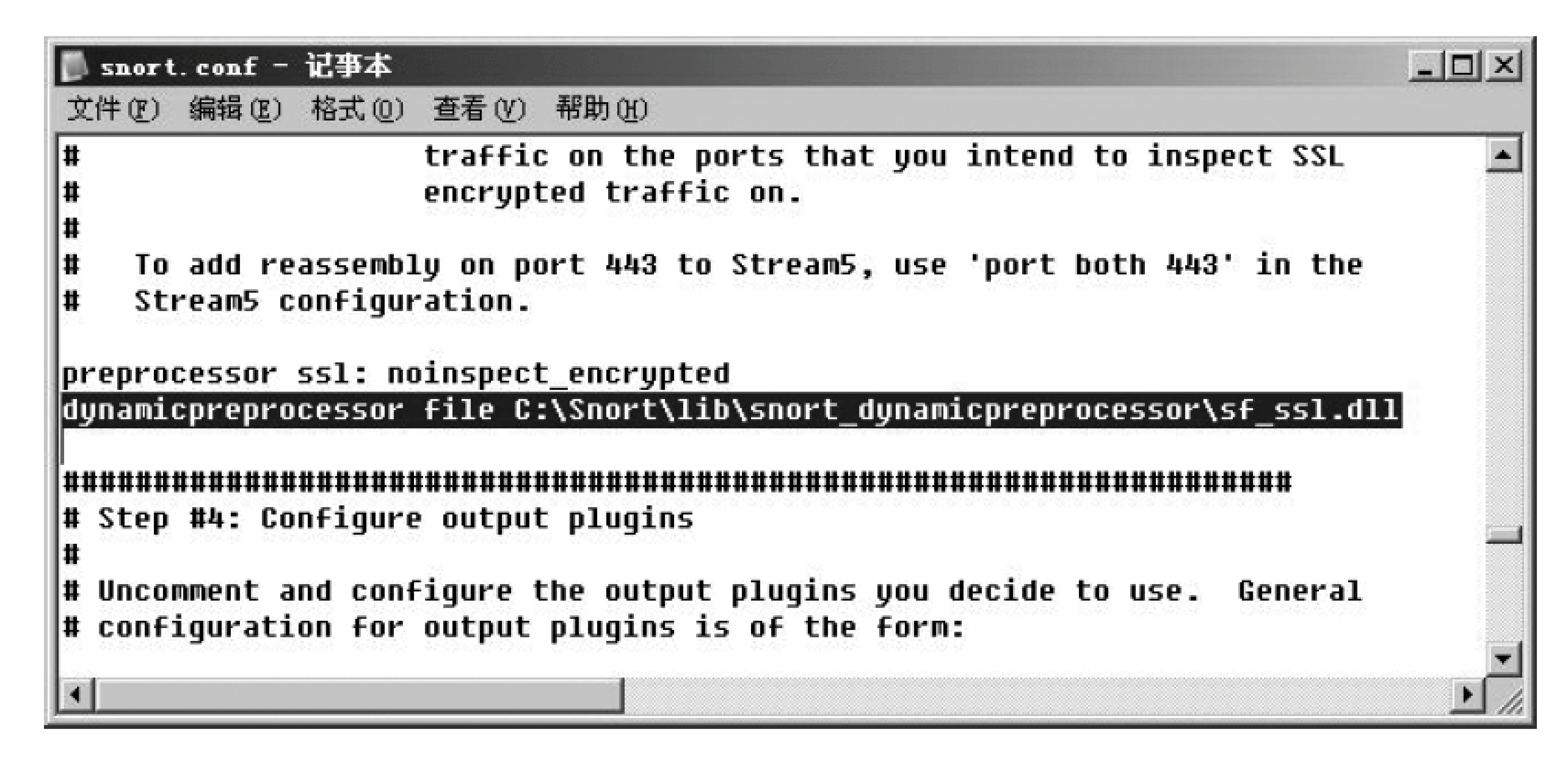
(6) 设置 Snort 输出 alert 到 MySQL Server,增加如下两行语句(图 6-37 和图 6-38):



```
snort.conf - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
#
# output database: log, mysql, user=root password=test dbname=db host=localhost
# output database: alert, postgresql, user=snort dbname=snort
# output database: log, odbc, user=snort dbname=snort
# output database: log, mssql, dbname=snort user=snort password=test
# output database: log, oracle, dbname=snort user=snort password=test
output database: alert, mysql, user=root password=123456 dbname=snort host=localhost port

# unified: Snort unified binary format alerting and logging
# -------------------------------------------------------------
# The unified output plugin provides two new formats for logging and generating
# alerts from Snort, the "unified" format.  The unified format is a straight
```

图 6-37　snort. conf 配置文件内容(二)



```
snort.conf - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
#                   traffic on the ports that you intend to inspect SSL
#                   encrypted traffic on.
#
#   To add reassembly on port 443 to Stream5, use 'port both 443' in the
#   Stream5 configuration.

preprocessor ssl: noinspect_encrypted
dynamicpreprocessor file C:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll

###########################################################################
# Step #4: Configure output plugins
#
# Uncomment and configure the output plugins you decide to use.  General
# configuration for output plugins is of the form:
```

图 6-38　snort. conf 配置文件内容(三)



```
output database: alert, mysql, user=root password=123456 dbname=snort host=localhost encoding
=hex detail=full
dynamicpreprocessor file C:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll
```

（7）保存 snort.conf 文件。

14．Windows 平台下 Snort 的使用

在命令行方式下输入如下命令：

```
C:\>set pcap_frames=max
C:\>cd\snort\bin
C:\snort\bin>snort-W
```

注意：每次重新启动 Snort，都要按类似上述方式正确输入 set pcap_frames=max 语句，否则执行上述的第 2、3 条语句后会出现 Not Using PCAP_FRAMES 错误提示。按上述方式启动 Snort 后，如果出现 using PCAP_FRAMES 提示，则说明一切配置正常。

（1）Snort 嗅探器模式。在命令行方式下输入如下命令：

```
C:\snort\bin>snort-v-i2
```

使 Snort 只将 IP 和 TCP/UDP/ICMP 的包头信息输出到屏幕上（图 6-39）。如果要看到应用层的数据，可以输入如下命令：

```
C:\snort\bin>snort-v-d-i2
```

如果需要输出更详细的信息，输入命令：

```
C:\snort\bin>snort-v-d-e-i2
```

可以显示数据链路层的信息。

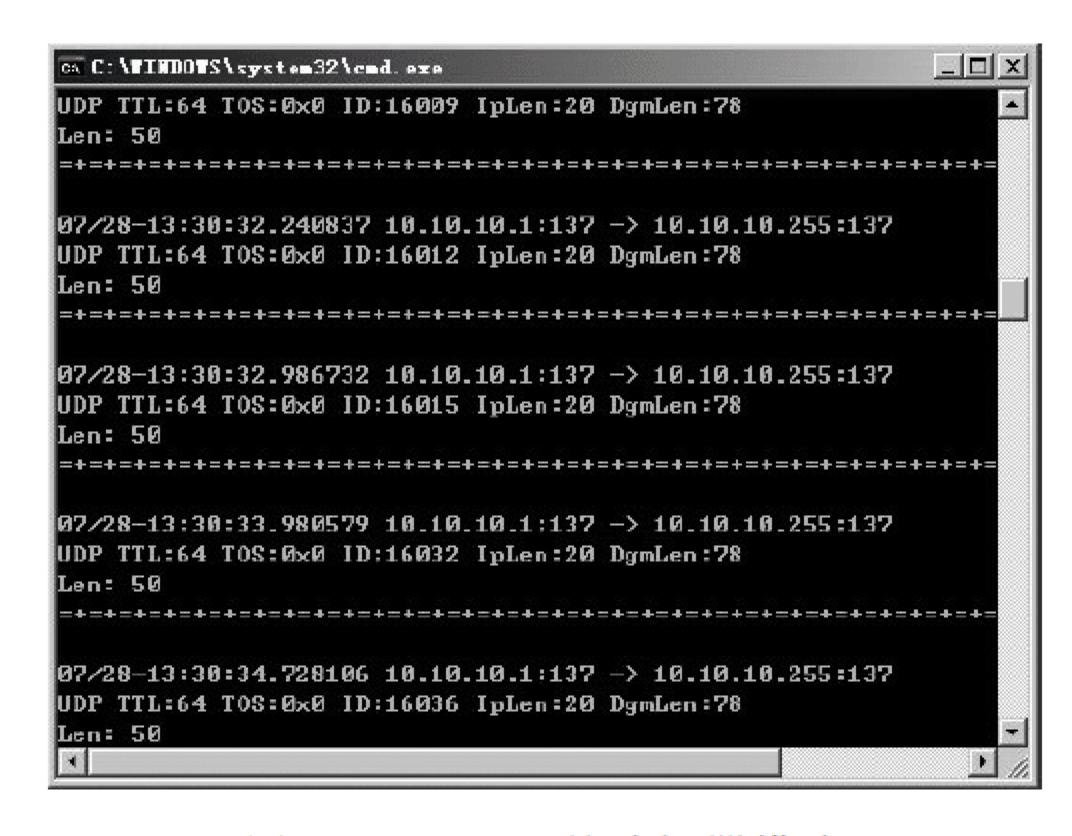


图 6-39　Snort 的嗅探器模式

（2）数据包记录器模式。上面的命令只是在屏幕上输出，如果要记录在 Log 文件上，需要预先建立一个 Log 目录。输入下面的命令启用数据包记录器模式：

```
C:\Snort\bin>snort-dve-i2-l C:\Snort\log-h 192.168.3.0/24-K ascii
```

其中，－l 选项指定存放日志的文件夹；－h 指定目标主机，这里检测对象是局域网段内的所有主机，如不指定－h，则默认检测本机；－K 指定了记录的格式，默认是 Tcpdump 格式，此处使用 ASCII 码（结果如图 6-40 所示）。在命令行窗口运行了该指令后，将打开保存日志的目录。

在 Log 目录下自动生成了多个文件夹，文件夹是以数据包目标主机的 IP 地址命名的（图 6-41），每个文件夹下记录的日志就是和该外部主机相关的网络流量。打开其中任一个，使用记事本查看日志文件，会发现文件的内容和嗅探器模式下的屏幕输出类似（见图 6-42）。



```
C:\WINDOWS\system32\cmd.exe
Using PCAP_FRAMES = max
07/22-00:38:39.666609 0:C:29:ED:81:FD -> FF:FF:FF:FF:FF:FF type:0x800
192.168.3.23:137 -> 192.168.3.255:137 UDP TTL:128 TOS:0x0 ID:2039 IpLe
n:78
Len: 50
81 8B 01 10 00 01 00 00 00 00 00 00 20 45 42 46   ............ EBF
45 45 46 45 4F 43 41 43 41 43 41 43 41 43 41 43   EEFEOCACACACACAC
41 43 41 43 41 43 41 43 41 43 41 42 4D 00 00 20   ACACACACACABM..
00 01                                             ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/22-00:38:40.413160 0:C:29:ED:81:FD -> FF:FF:FF:FF:FF:FF type:0x800
192.168.3.23:137 -> 192.168.3.255:137 UDP TTL:128 TOS:0x0 ID:2040 IpLe
n:78
Len: 50
81 8B 01 10 00 01 00 00 00 00 00 00 20 45 42 46   ............ EBF
45 45 46 45 4F 43 41 43 41 43 41 43 41 43 41 43   EEFEOCACACACACAC
41 43 41 43 41 43 41 43 41 43 41 42 4D 00 00 20   ACACACACACABM..
00 01                                             ..
```

图 6-40　Snort 数据包记录器模式

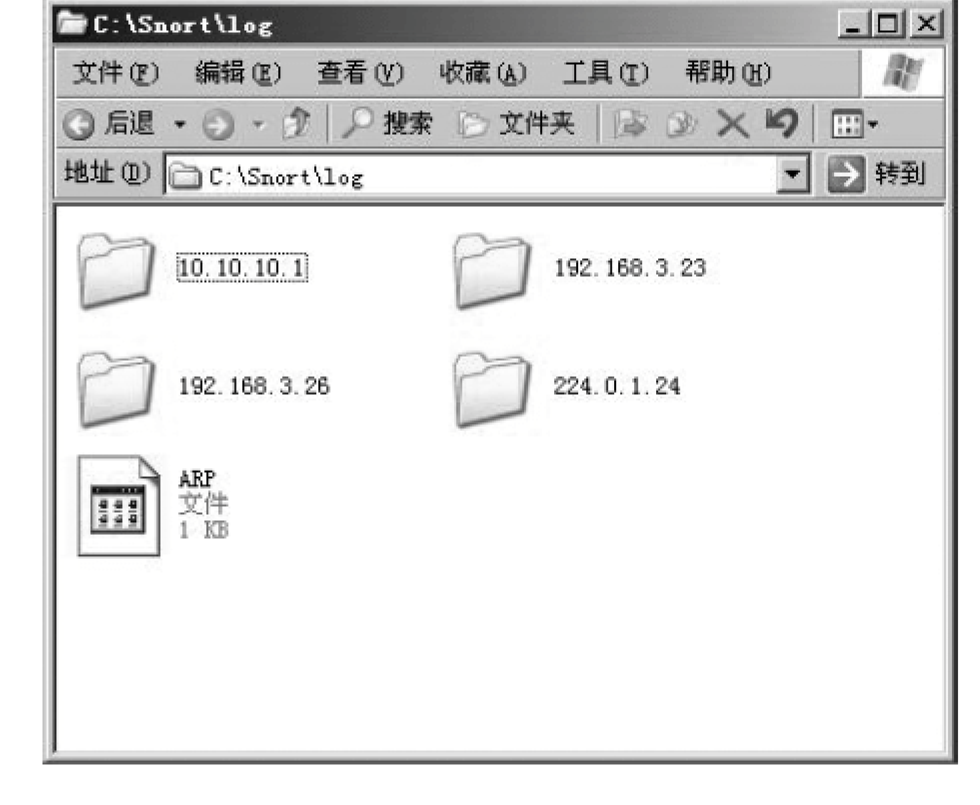
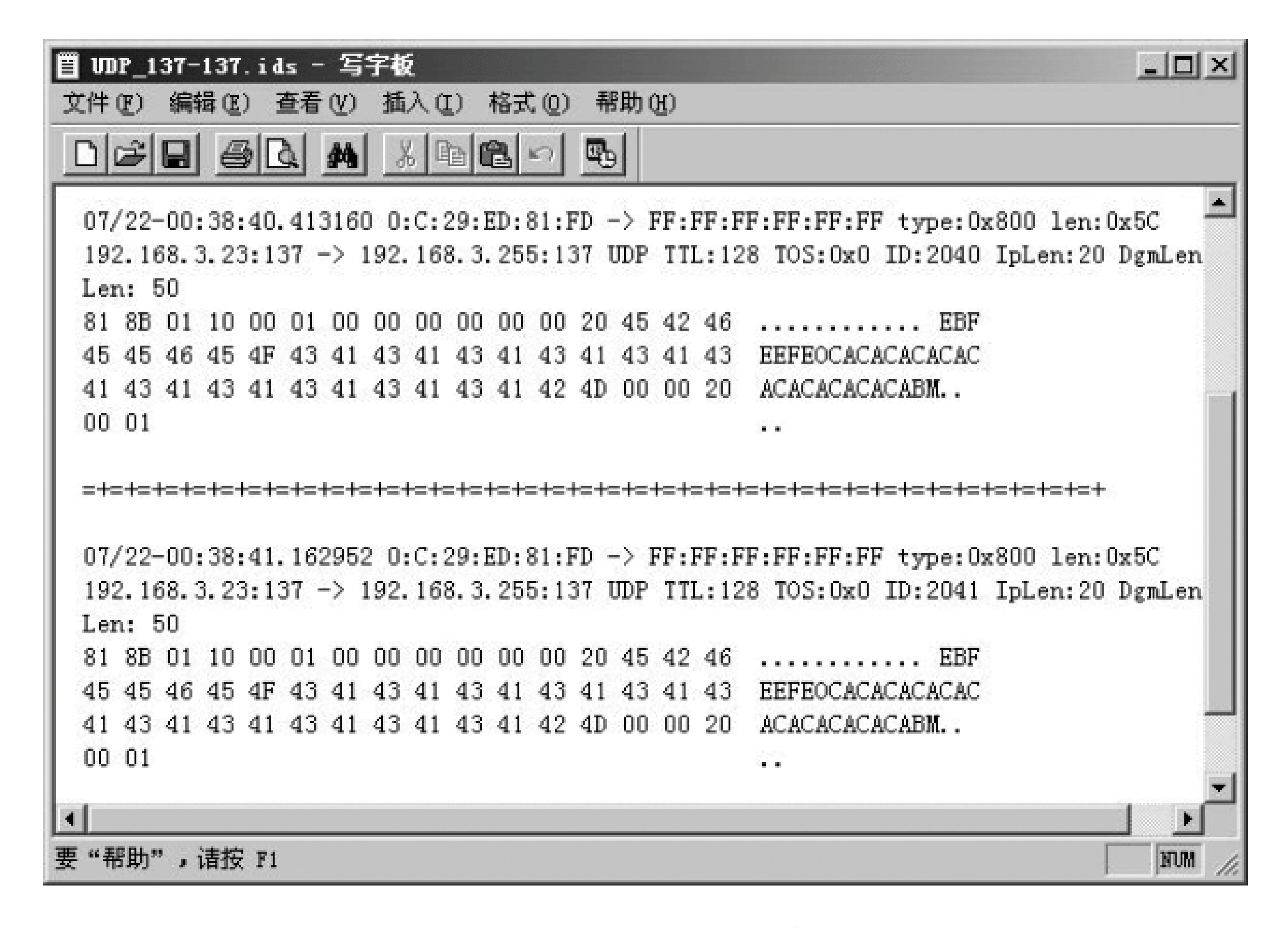


图 6-41　Snort 数据包记录器模式记录的日志



UDP_137-137.ids - 写字板

文件(F) 编辑(E) 查看(V) 插入(I) 格式(O) 帮助(H)

```
07/22-00:38:40.413160 0:C:29:ED:81:FD -> FF:FF:FF:FF:FF:FF type:0x800 len:0x5C
192.168.3.23:137 -> 192.168.3.255:137 UDP TTL:128 TOS:0x0 ID:2040 IpLen:20 DgmLen
Len: 50
81 8B 01 10 00 01 00 00 00 00 00 00 20 45 42 46   ............ EBF
45 45 46 45 4F 43 41 43 41 43 41 43 41 43 41 43   EEFEOCACACACACAC
41 43 41 43 41 43 41 43 41 43 41 42 4D 00 00 20   ACACACACACABM..
00 01                                             ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/22-00:38:41.162952 0:C:29:ED:81:FD -> FF:FF:FF:FF:FF:FF type:0x800 len:0x5C
192.168.3.23:137 -> 192.168.3.255:137 UDP TTL:128 TOS:0x0 ID:2041 IpLen:20 DgmLen
Len: 50
81 8B 01 10 00 01 00 00 00 00 00 00 20 45 42 46   ............ EBF
45 45 46 45 4F 43 41 43 41 43 41 43 41 43 41 43   EEFEOCACACACACAC
41 43 41 43 41 43 41 43 41 43 41 42 4D 00 00 20   ACACACACACABM..
00 01                                             ..
```

要"帮助"，请按 F1　　NUM

图 6-42　日志文件

(3) 网络 IDS 模式。Snort 最重要的用途还是作为基于误用检测技术的 NIDS。下面将通过对运行了 Snort 的目标主机进行有意攻击，来观察 Snort 检测入侵的能力。首先，向目标主机发送 ICMP 长数据包来观测 Snort 的反映，ICMP 长数据包是有潜在危险的，一般会被视为入侵；然后，使用网络端口扫描工具 Nmap 对目标主机进行扫描，观察 Snort 的检测情况。具体操作步骤如下：

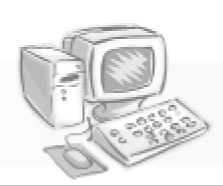
① 打开 C:\Snort\rules 文件夹中的 Icmp.rules 文件，增加如下一条规则，该规则用于检测 ICMP 长数据包(图 6-43)：

```
alert icmp $ EXTERNAL_NET any -> $ HOME_NET any (msg:"ICMP Large ICMP Packet";dsize:> 800;
reference:arachnids,246;classtype:bad-unknown;sid:499;rev:4;)
```

② 打开 C:\Snort\rules 文件夹中的 scan.rules 文件，将下列规则前面的"#"号删除，该规则用于检测 SCAN 扫描(图 6-44)。

```
alert tcp $ EXTERNAL_NET any -> $ HOME_NET any (msg:"SCAN XMAS";flow:stateless;flags:SRAFPU,
12;reference:arachnids,144;classtype:attempted-recon;sid:625;rev:7;)
```





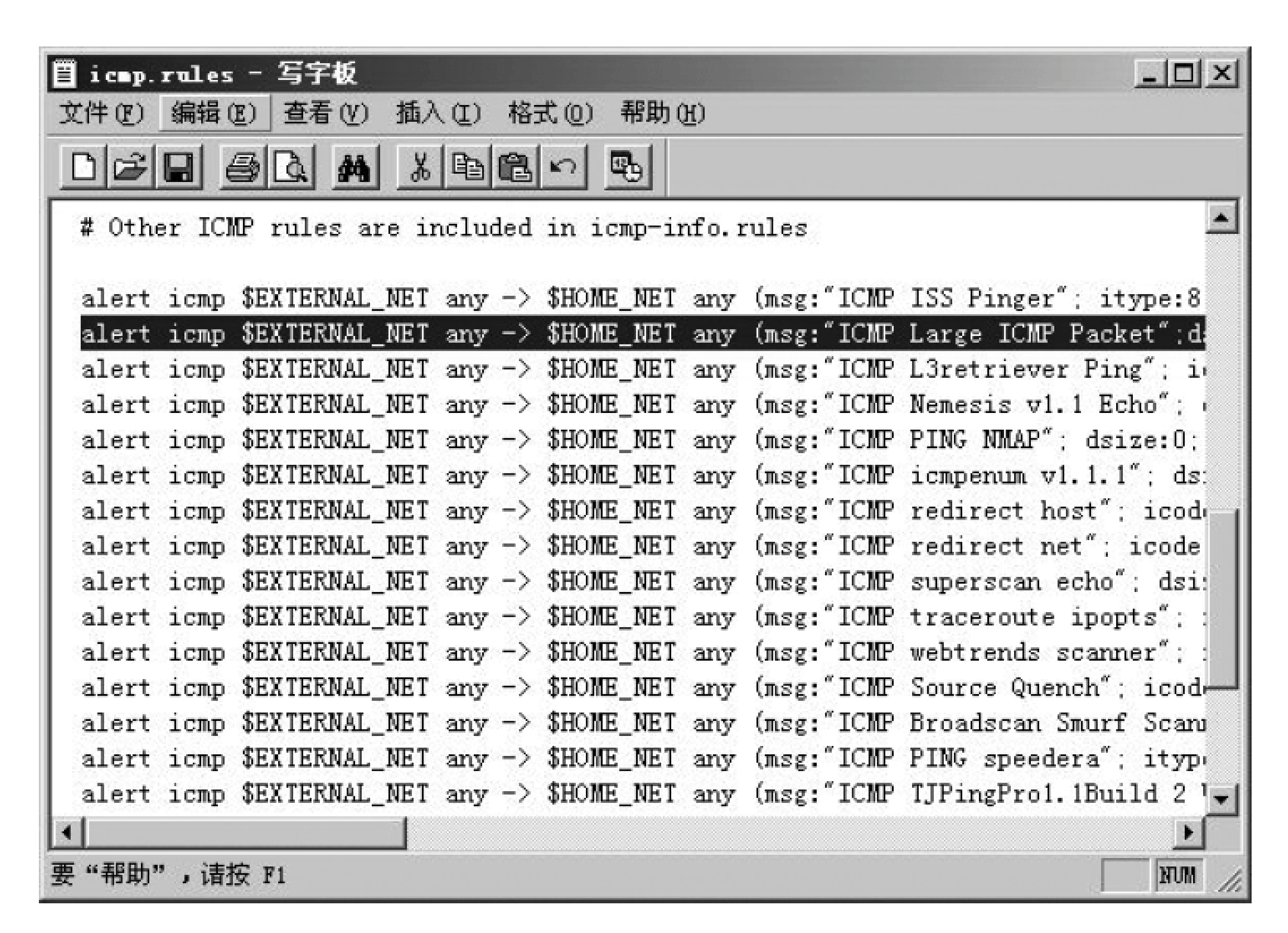


图 6-43 ICMP 长数据包对应的检测规则



图 6-44 SCAN 扫描对应的检测规则

③ 输入下面的命令启动 IDS 模式：

```
C:\Snort\bin> snort- i2- dev- l../log- h 192.168.3.0/24- K ascii- c C: /Snort/etc/snort.conf
```

相比数据包记录器模式中使用的命令，该命令只增加了一个选项－c，用于告诉 Snort 使用 Snort.conf 中的规则集文件。Snort 会对每个包和规则集进行匹配，如符合规则，就采取规则所指定的动作。

④ 在局域网的另一台主机(192.168.3.26)上向目标主机发送数据包，输入下面的命令：

```
C:\>ping – l 65423 192.168.0.20
```



⑤ 目标主机中可以检测到这次探测的数据包(图 6-45)。在目标主机中打开 Log 文件夹,此时可以发现在 Log 的根目录下自动生成了一个名为 Alert 的文件。使用写字板打开该文件并观察其内容(图 6-46)。Snort 警报中记录了刚才发送的 ICMP 长数据包,其中每条记录包括警报的类型和数据包的包头。发送的 ICMP 长数据包之所以出现在警报中,是因为它的特征和 Snort 预先定义的规则相符。

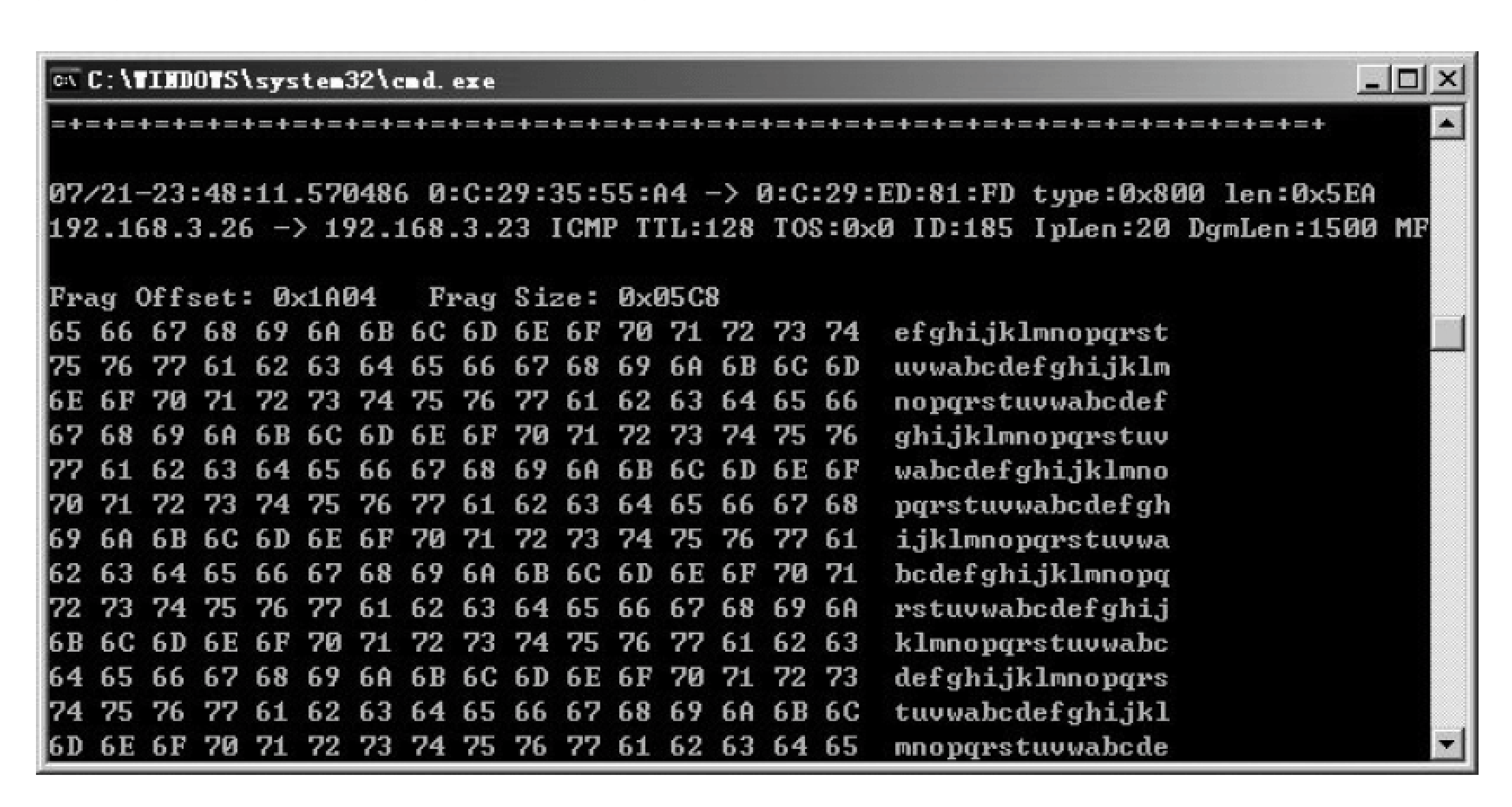


图 6-45　检测到探测的数据包

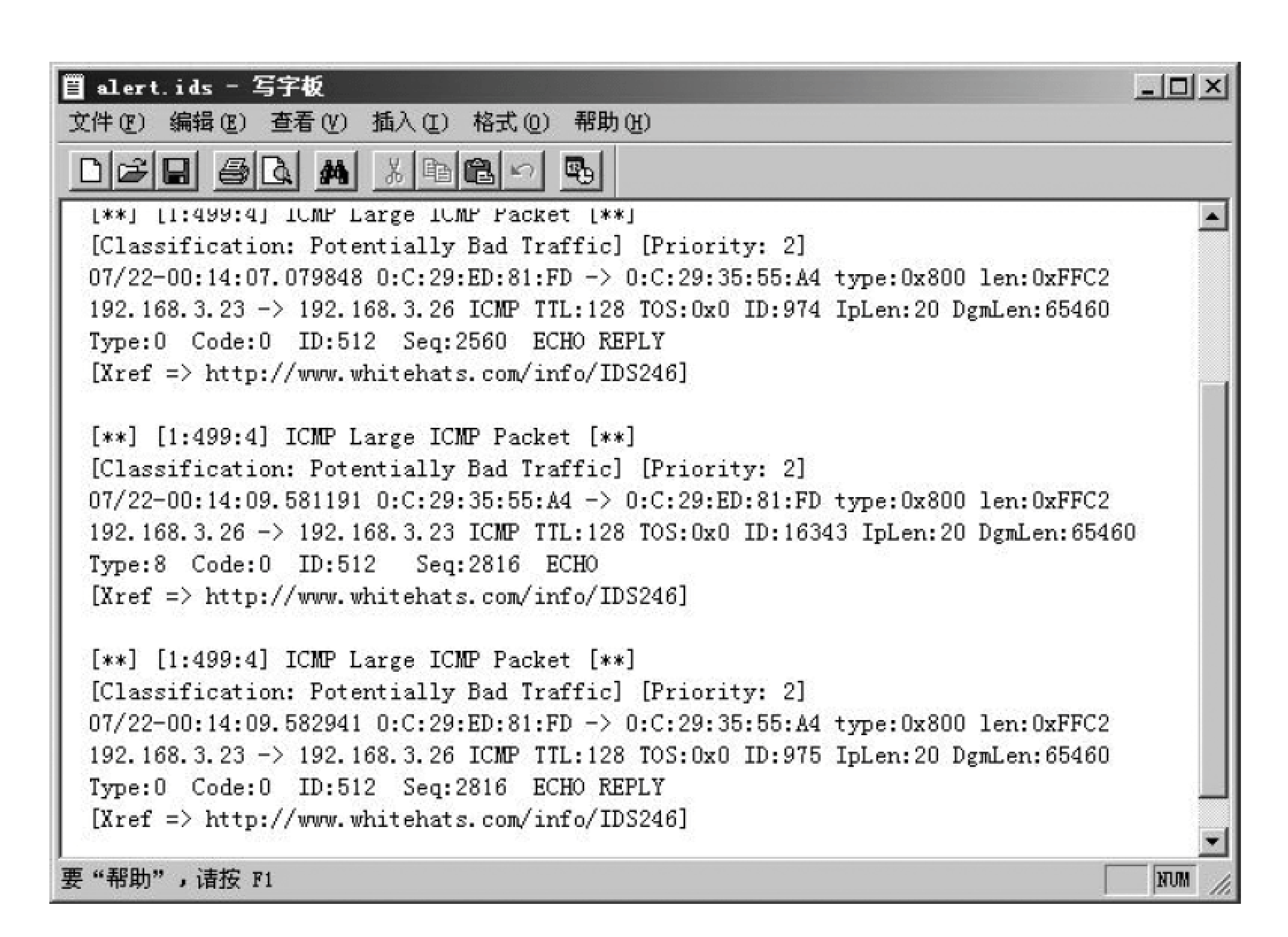
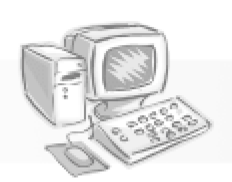


图 6-46　Snort 记录的 ICMP 警报

⑥ 执行端口扫描的检测。把 Snort.conf 文件中相应端口配置部分的内容修改为如图 6-47 所示的值。其中 proto 指定了需要检测的协议类型,包括 TCP、UDP、ICMP 和 IP,all 表示检测所有的协议;sense_level 指定检测的灵敏度,灵敏度高可以增加检测率,但有可能会同时增加误报率,Snort 的默认选项是 Low;logfile 指定检测结果的输出文件名(设文件名为 outscan),该文件将创建在 Log 目录下。

⑦ 在局域网的另一台主机(192.168.3.26)上安装并运行 Nmap,对目标主





机(192.168.3.23)进行扫描，探测到了多个开放端口(图 6-48)。

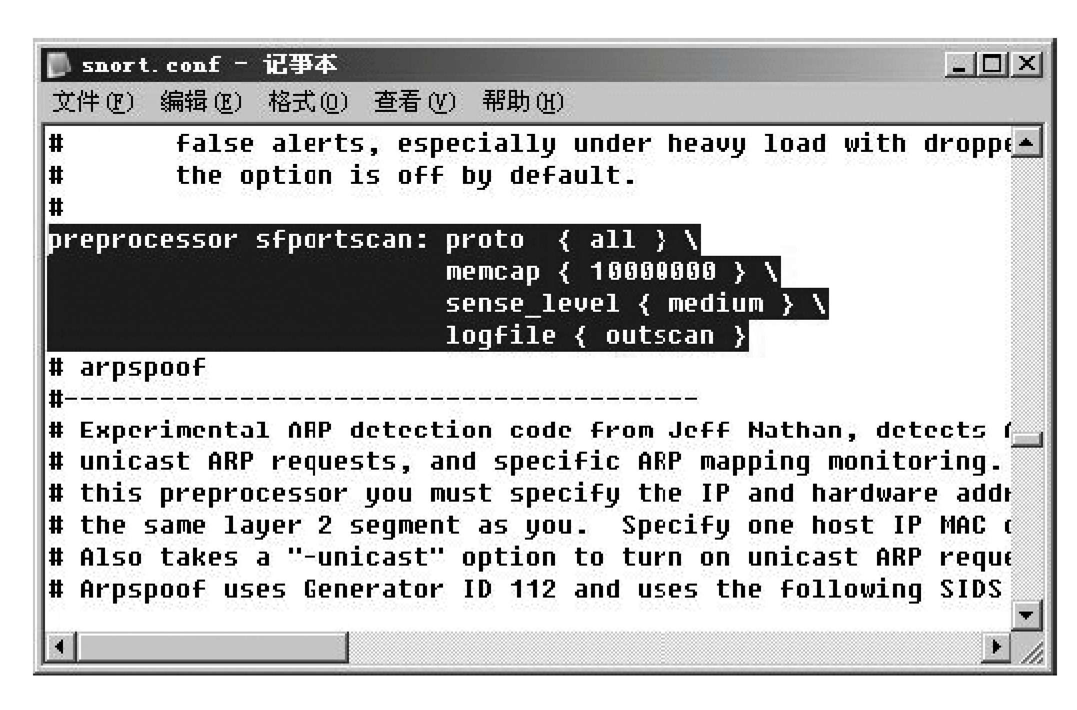


图 6-47　配置 Snort 的端口扫描选项

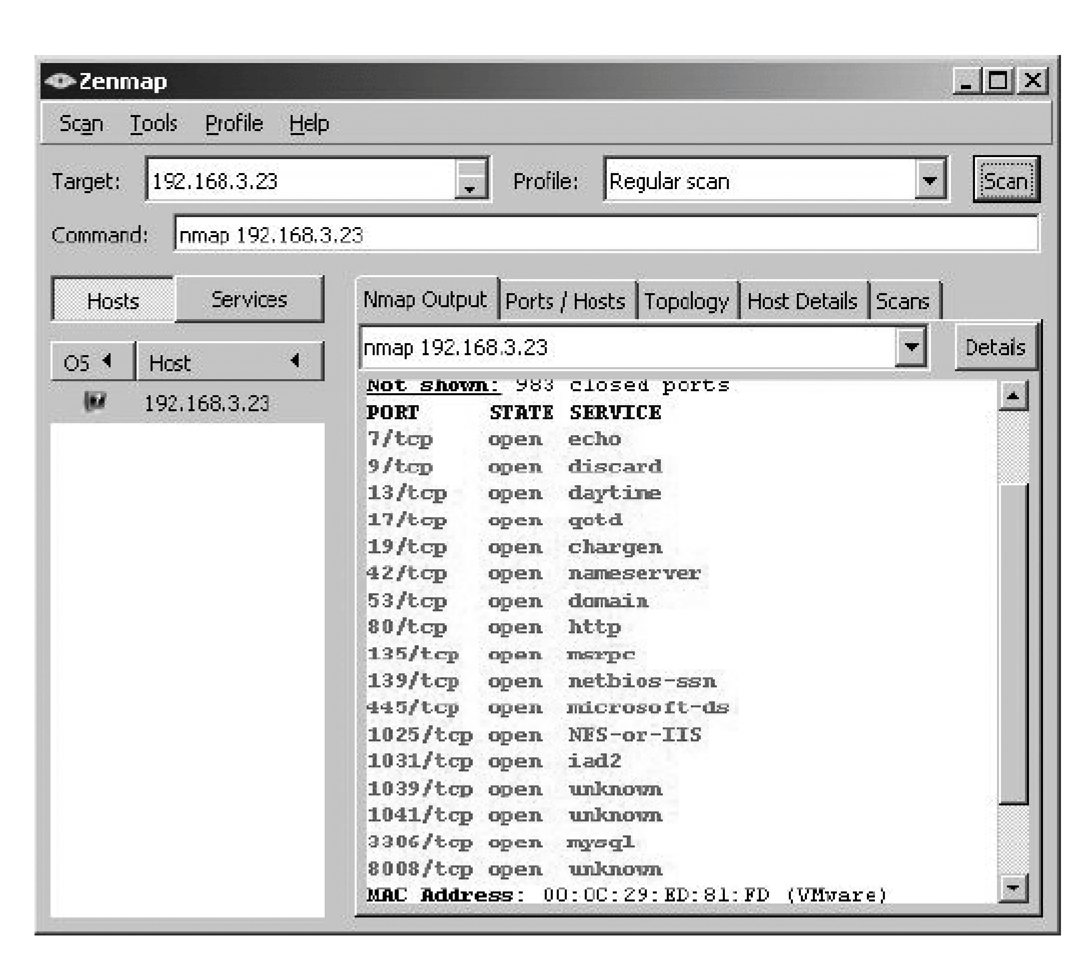


图 6-48　对运行 Snort 的主机进行端口扫描

⑧ 在目标主机上查看记录端口扫描检测结果的文件 outscan(图 6-49)。可以看出，Snort 准确地识别并分析记录了端口扫描攻击相关的信息，如攻击者的 IP 地址是 192.168.3.26，扫描的范围从 21 号端口到 32780 号端口。

⑨ 打开 Alarm 文件(图 6-50)，发现在 Alarm 文件里增加了与端口扫描相关的警告。Alarm 文件中记录的是单个数据包和规则匹配的结果。



图 6-49　Snort 端口扫描检测结果

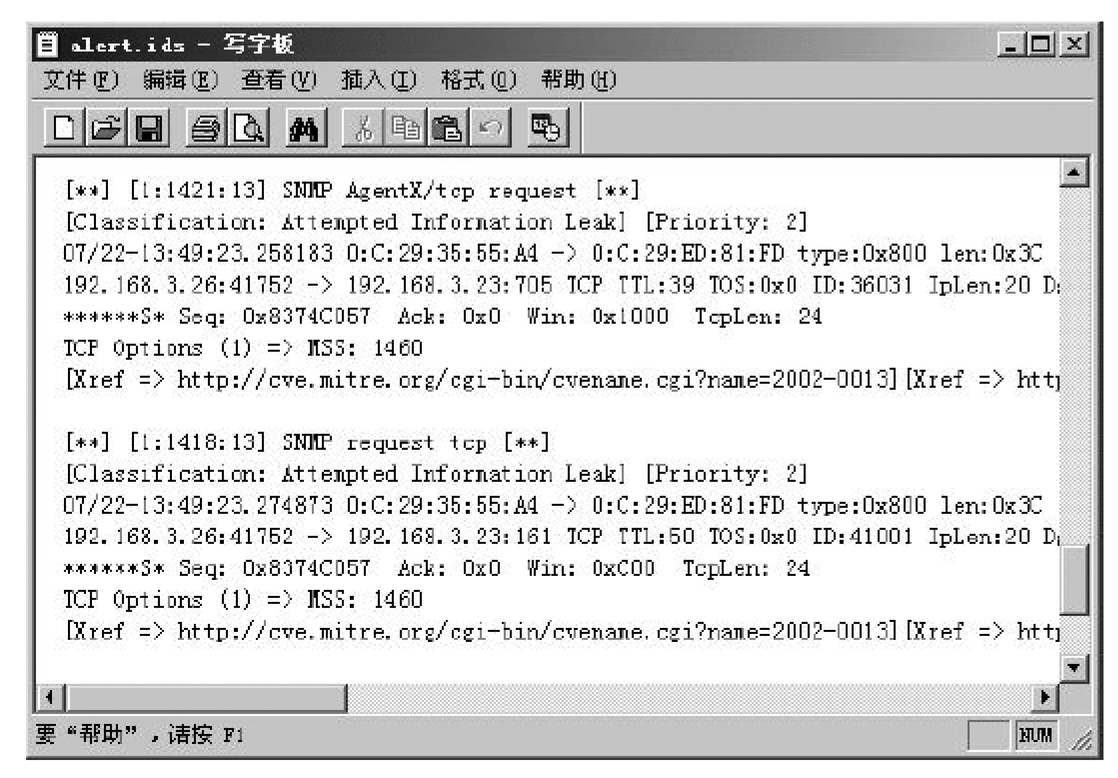


图 6-50　Snort 对端口扫描攻击的警报

15. 查看统计数据

在 IE 浏览器的地址栏输入：http://localhost:8008/acid/acid_main.php，可以查看统计数据(图 6-51)。

6.6　入侵防御系统概述

随着网络攻击技术的不断提高和网络安全漏洞的不断发现，人们也逐渐意识到 IDS 所面临的问题：IDS 系统在识别大规模的组合式、分布式的入侵攻击方面，还没有较好的方法



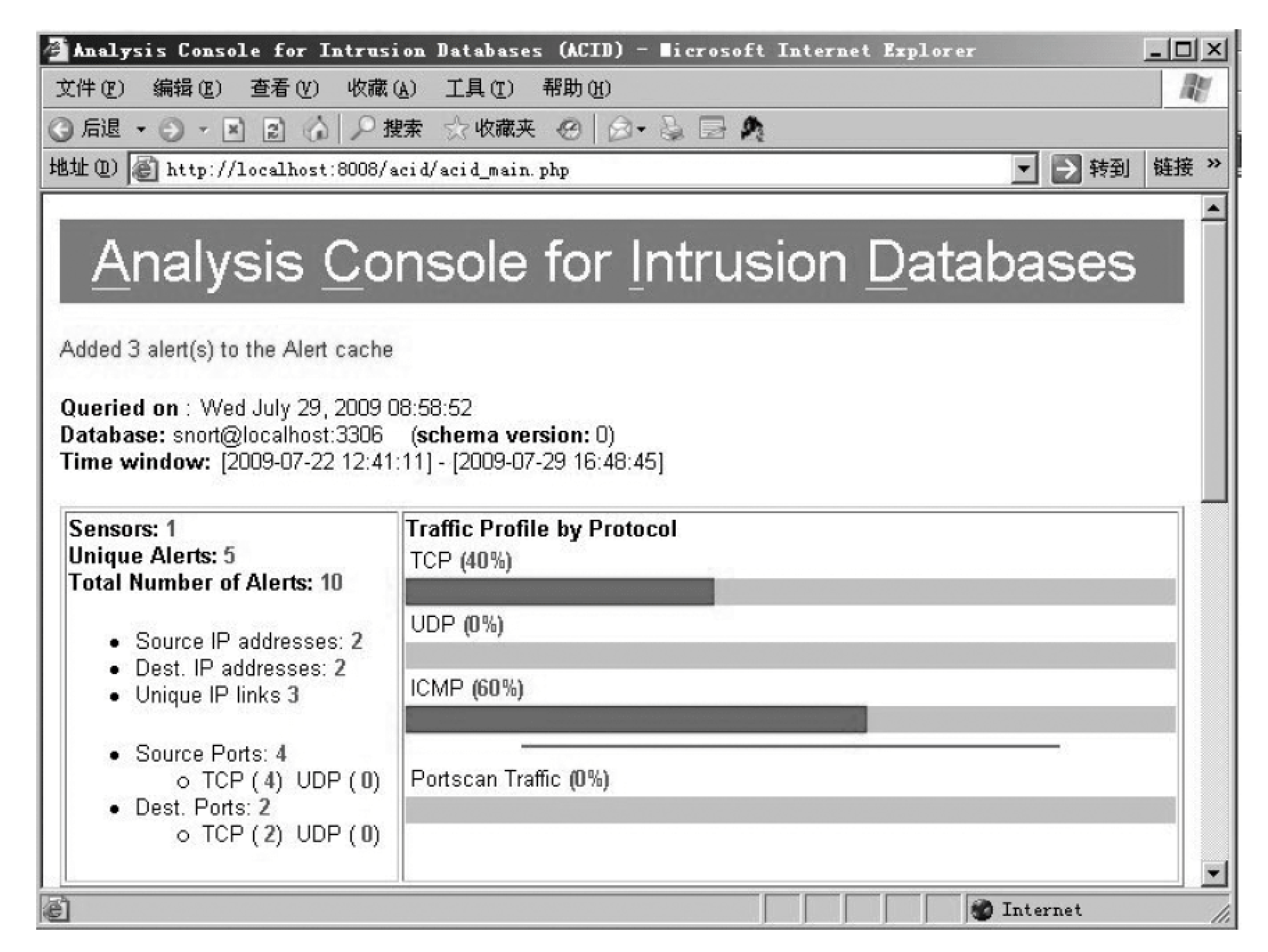


图 6-51 统计数据

和成熟的解决方案，误报与漏报现象严重，用户往往淹没在海量的报警信息中，而漏掉真正的报警；此外，IDS 只能报警而不能有效采取阻断措施的设计理念，也不能满足用户对网络安全日益增长的需求。

《信息周刊》研究部和国际商业机器公司(IBM)合作进行了 2008 年“中国信息安全调查”，63.9%的企业表示：通常都是在系统资源无法正常运行和服务，声誉和资产都遭到损失时，才得知受到攻击。安永会计师事务所上海分所科技与信息安全咨询服务部合伙人阮祺康讲述了这样一个案例：黑客对某大型零售商的交易系统不断进行攻击，然而该公司始终没有发现黑客入侵的迹象，最终导致数千万顾客的信用卡和借记卡信息泄露，累计损失达到了数百万美元。

由此可见，从被动防御到主动防御，正成为企业当前面临的新考验。入侵防御系统(Intrusion-prevention system，IPS)正是一种主动、机智的防御系统，它的拦截行为与其分析行为处在同一层次，能够更敏锐地捕捉入侵的流量，并能将危害切断在发生之前。

6.6.1 入侵防御系统的特征

IPS 具有以下四大特征。

1. 以嵌入模式运行

只有以嵌入模式运行的 IPS 产品才能够实现实时的安全防护，实时阻拦所有可疑的数据包，并对该数据流的剩余部分进行拦截。



2. 深入分析能力

IPS具有深入分析能力，以确定哪些恶意流量已经被拦截，根据攻击类型、策略等来确定哪些流量应该被拦截。

3. 高质量的攻击行为特征库

IPS要依靠各种攻击行为特征来对数据包分类和过滤，所以高质量的攻击行为特征库是IPS高效运行的必要条件，IPS还应该定期升级攻击行为特征库，并快速应用到所有传感器。但是就目前来看，绝大多数IPS产品在这方面做得还不够，存在许多误报行为，造成日志记录过多，影响IPS产品性能的正常发挥。同时也增加了网络管理员的管理负担。

4. 高效的处理能力

IPS不仅要对所有数据包进行分类并检测，还要对可疑数据包进行拦截，因此它必须具有高效地处理数据包的能力，使之对整个网络性能的影响降低到最小。

6.6.2 入侵防御系统的工作原理

为了正确理解IPS的工作原理和它所具有的优势，首先从传统的防火墙和IDS防御机制进行比较。防火墙是实施访问控制策略的系统，主要对流经的OSI第2～4层(也有基于OSI第7层的)网络流量进行检查，拦截不符合安全策略的数据包，旨在拒绝那些明显可疑的网络流量，但仍然允许某些基于OSI高层的流量通过，因此防火墙对于很多应用型攻击仍然无计可施。

IDS是通过监视网络或系统资源，寻找违反安全策略的行为或攻击迹象，发现后发出报警。所以IDS只是一套报警系统，并不具有真正的防御和阻止攻击的能力，而且IDS系统是被动的，也就是说，在攻击实际发生之前，它们往往无法预先发出警报。

IPS则能提供对OSI第2～7层的全面主动防御，其设计宗旨是预先对入侵活动和攻击性网络流量进行拦截，避免其造成损失，而不是简单地在恶意流量传送时或传送后才发出警报。IPS主要包括检测和防御两大系统。理想的IPS应具备从网络到主机的防御措施及预设定的响应设置，通常由IDS和防火墙技术分别发展组合而成。检测和实时防御是IP的最重要的性能特征。IPS是通过直接嵌入到网络流量中实现这两种功能的，即通过一个网络端口接收来自外部系统的流量，经过检查确认其中不包含异常活动或可疑内容后，再通过另外一个端口将它传送到内部系统中。这样一来，有问题的数据包，以及所有来自同一数据流的后续数据包，都能在IPS设备中被清除掉。它的基本工作原理如图6-52所示。

首先，数据包在流入IPS设备前要进行数据包分类，依据就是数据包中的报头信息，如源IP地址和目的IP地址、端口号和应用域，对于不完整或者不符合分类标准的数据包将被丢弃。通过的数据进入对应的过滤器，根据过滤器中所设置的不同攻击行为特征进行数据包检查，如果符合其中的攻击行为特征，则把相应数据包标记为“命中”。被标记为“命中”的数据包将在随后的出口处被丢弃，其余的数据包将通过出口进入内部网络。同时，把被标记



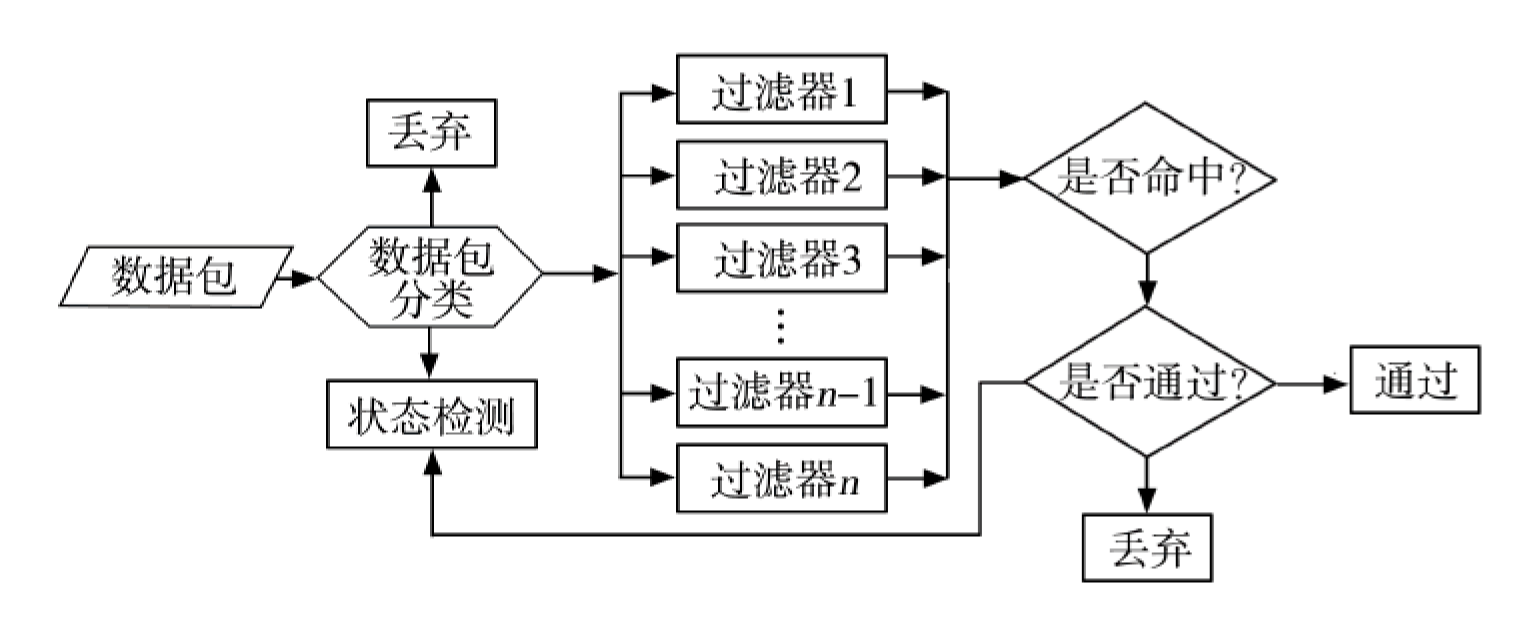


图 6-52 IPS 工作原理图

为“命中”的数据包特征在“状态检测”功能特征库中进行更新，这样下次在数据包分类过程中就可以把这些数据包丢弃，不再进入过滤器，进一步提高了数据包过滤的效率，更有效地阻止了攻击行为。

IPS 实现实时检查和阻止入侵的原理在于 IPS 拥有许多针对不同攻击行为特征设计的过滤器，能够防止各种攻击行为。针对不同的攻击行为，IPS 需要不同的过滤器，每种过滤器都设有相应的过滤规则。为了确保准确性，这些规则的定义非常广泛。在对传输内容进行分类时，过滤引擎还需要参照数据包的信息参数，并将其解析至一个有意义的域中进行上下文分析，以提高过滤的准确性。当新的攻击手段被发现之后，IPS 就会创建一个新的过滤器。

过滤器引擎集合了流水和大规模并行处理硬件，能够同时执行数千次的数据包过滤检查。并行过滤处理可以确保数据包能够不间断地快速通过系统，不会对速度造成影响。这种硬件加速技术对于 IPS 具有重要的意义，因为传统的软件解决方案必须串行进行过滤检查，会导致系统性能大打折扣。

IPS 数据包处理引擎是专业化定制的集成电路，可以深层检查数据包的内容。如果有攻击者利用 OSI 第 2～7 层的漏洞发起攻击，IPS 能够从数据流中检查出这些攻击并加以阻止。传统的防火墙大多数只能对第 3 层或第 4 层进行检查，不能检测应用层的内容。防火墙的包过滤技术不会针对每一字节进行检查，因而也就无法发现攻击活动，而 IPS 可以做到逐一字节地检查数据包。

6.6.3 入侵防御系统的分类

与 IDS 一样，随着 IPS 技术的发展和应用的深入，目前 IPS 产品也出现了不同类型，并应用于不同的环境中。主要分为以下两类。

1. 基于主机的入侵防御系统(Host Intrusion Prevent System，HIPS)

HIPS 通过在主机/服务器上安装软件代理程序，防止网络攻击入侵操作系统以及应用程序。基于主机的入侵防御功能能够保护服务器的安全弱点不被不法分子所利用。Cisco 公司的 Okena、NAI 公司的 McAfee Entercept、冠群金辰的龙渊服务器核心防护都属于这类产品。HIPS 可以根据自定义的安全策略以及分析学习机制来阻断对服务器、主机发起的恶意入侵；阻断缓冲区溢出、改变登录口令、改写动态链接库以及其他试图从操作系统夺



取控制权的入侵行为，整体提升主机的安全水平。

在技术上，HIPS采用独特的服务器保护途径，利用由包过滤、状态包检测和实时入侵检测组成分层防护体系。这种体系能够在提供合理吞吐率的前提下，最大限度地保护服务器的敏感内容，既可以以软件形式嵌入到应用程序对操作系统的调用当中，通过拦截针对操作系统的可疑调用，提供对主机的安全防护；也可以以更改操作系统内核程序的方式，提供比操作系统更加严谨的安全控制机制。

由于HIPS工作在受保护的主机/服务器上，它不但能够利用特征和行为规则检测，阻止诸如缓冲区溢出之类的已知攻击，还能够防范未知攻击，防止针对Web页面、应用和资源未授权的任何非法访问。HIPS与具体的主机/服务器操作系统平台紧密相关，不同的平台需要不同的软件代理程序。

2. 基于网络的入侵防御系统(Network Intrusion Prevent System，NIPS)

随着新型网络蠕虫(Slammer LovSan等)的出现，它不通过网页下载或是邮件传送来散布，而是采用如SQL and RPC(结构化查询语言和远程过程调用)来进行攻击，目标是网络上已知系统漏洞的计算机。由于系统管理员无法全天24小时随时监控，因此NIPS是比较适当的方法，其采取的机制如下：丢弃封包(packet drop)、封锁来源(source blocking)、重导联机(onnection reset)、会话代理(session proxy)等。NIPS通过检测流经的网络流量，提供对网络系统的安全保护，可以做到实时的阻挡黑客的入侵行为以及破坏行为。另外，由于NIPS采用在线连接方式，一旦辨别出入侵行为，NIPS就可以取消该入侵通信的整个网络会话，而不仅仅是复位会话。

在技术上，NIPS吸取了目前NIDS所有的成熟技术，包括特征匹配、协议分析和异常检测。特征匹配是最广泛应用的技术，具有准确率高、速度快的特点。基于状态的特征匹配不但检测攻击行为的特征，还要检查当前网络的会话状态，避免受到欺骗攻击。协议分析是一种较新的入侵检测技术，它充分利用网络协议的高度有序性，并结合高速数据包捕捉和协议分析来快速检测某种攻击特征。协议分析正在逐渐进入成熟应用阶段，协议分析能够理解不同协议的工作原理，以此分析这些协议的数据包，寻找可疑或不正常的访问行为。协议分析不仅仅基于协议标准(如RFC)，还基于协议的具体实现，这是因为很多协议的实现偏离了协议标准。通过协议分析，IPS能够针对插入(Insertion)与规避(Evasion)攻击进行检测。异常检测的误报率比较高，NIPS不将其作为主要技术。

由于要实时在线，NIPS需要具备很高的性能，以免成为网络的瓶颈，因此，NIPS通常被设计成类似于交换机的网络设备，提供线速吞吐率以及多个网络端口。NIPS必须基于特定的硬件平台，才能实现千兆位级网络流量的深度数据包检测和阻断功能。这种特定的硬件平台通常可以分为3类：一类是网络处理器(网络芯片)，另一类是专用的FPGA编程芯片，第三类是专用的ASIC芯片。

NIPS的实时检测与阻断功能很有可能出现在未来的交换机或者防火墙上。随着处理器性能的提高，每一层次的交换机都有可能集成入侵防护功能。也有专家预测，NIPS就是下一代的防火墙。



6.6.4 典型入侵防御产品介绍

1. 天清入侵防御系统

天清入侵防御系统(简称：天清 IPS,如图 6-53 所示)是启明星辰信息技术有限公司自行研制开发的入侵防御类网络安全产品。该产品不仅可以对网络蠕虫、间谍软件、溢出攻击、数据库攻击、网络设备攻击等多种深层攻击行为进行主动阻断,弥补其他安全产品深层防御效果的不足,同时也融入了启明星辰公司在入侵攻击识别方面的积累和研究成果,在精确阻断方面达到国际领先水平。

天清 IPS 产品有如下特点：

- 精确阻断达到国际领先水平：天清 IPS 融合了基于攻击躲避原理的阻断方法与基于攻击特征的阻断方法,不但有效提高了对各种深层攻击行为的识别能力,而且对攻击变种、SQL 注入等无法通过特征判断的攻击行为也能实现精确阻断。
- 在线部署,高效可靠：天清 IPS 是以透明方式串行部署于网络中。通过软、硬件双 Bypass 功能,即使在最恶劣的情况下,天清 IPS 也不会成为网络的故障点。天清 IPS 通过合理分配资源、CPU 与任务绑定等技术,大幅提升了系统的性能,其微秒级时延和千兆高吞吐量可满足电信级业务的应用。
- 综合管理,易用、易查：天清 IPS 支持向导式的策略配置管理,可根据需求灵活调整保护策略,达到最佳防御效果,并提供对历史记录信息细致的查询分析功能。
- 支持在线更新,防御最新威胁：天清 IPS 可通过在线自动升级,增加对最新威胁的防御能力。

2. 华为入侵防御系统

华为 3Com 公司最新推出的 TippingPoint 系列 IPS(图 6-54),具备对 OSI 第 2～7 层流量的深度分析与检测能力,同时配合以精心研究的攻击特征知识库和用户规则,既可以有效检测并实时阻断隐藏在海量网络流量中的病毒、攻击与滥用行为,也可以对分布在网络中的各种流量进行有效管理,从而达到对网络基础设施的保护、对网络应用的保护和对网络性能的保护。



图 6-53　天清入侵防御系统设备



图 6-54　华为入侵防御系统设备

TippingPoint IPS 产品有如下特点。

- 安全与高性能的结合：TippingPoint IPS 产品将统一的安全功能与出色的数据交换融合在一起,专门设计的硬件平台,使得其具备了类似以太网交换机的性能;采用基

于专业 ASIC 技术以及高性能网络处理器(NP)开发的威胁抑制引擎(Threat Suppression Engine，TSE)具备高达20GB的高带宽背板，提供大规模并行处理机制，TSE 可以对一个报文同时进行几千种检测，空前提高了整体的处理性能，TSE 还具备超强的流量分类、流量管理和流量整形功能，可以自动统计和计算正常状况下网络内各种应用流量的分布，并且基于该统计形成流量框架模型；当大量的 P2P、IM 流量侵占带宽等异常发生时，TSE 将根据已经建立的流量框架模型限制或者丢弃异常流量，保证关键业务的可达性和通畅性。

- 主动防御的网络安全：TippingPoint IPS 在跟踪流状态的基础上，可以在蠕虫、病毒、木马、DoS/DDoS、后门、Walk-in 蠕虫、连接劫持、带宽滥用等威胁发生前成功地检测并阻断；能够有效抵御针对路由器、交换机、DNS 服务器等网络重要基础设施的攻击；支持基于访问控制列表、统计、协议跟踪等检测机制，可以对流量进行细微粒度的识别与控制，有效检测流量浪涌、缓冲区溢出、漏洞利用、IPS 躲避等一些已知的、甚至未知的攻击。
- 升级维护轻松及时：TippingPoint 业界领先的专业安全威胁分析团队是安全威胁公告牌 SANS @Risk 的主导者与主要贡献人，SANS @Risk 每周四定期向其全球范围内 30 万专业订户发布披露最新安全威胁的公告，公告内容包含最新发现的漏洞、漏洞所带来的影响、表现形式以及指导用户如何采取防范措施。由此，TippingPoint 安全威胁分析团队将实时为所有 IPS 用户发布名为数字疫苗(Digital Vaccine，DV)的更新防护信息。不仅如此，TippingPoint 安全分析团队还与全球著名的系统软件厂商，如 Microsoft、Oracle 等，保持了良好的合作关系。在某个漏洞被发现后，TippingPoint 能够在第一时间(即厂商公布安全公告之前)获得该漏洞的详细信息，并且利用这一时间差及时制作可以抵御该漏洞的数字疫苗，使得用户的网络免遭这种“即时攻击”(Zero-day Attack)。
- 轻松管理：为满足不同类型用户对 IPS 产品部署与管理的需求特点，TippingPoint IPS 提供如下三种不同的操作管理方式。

  ✍ SMS-Security Management System，即面向规模部署的企业级综合管理中心。
  ✍ LSM-Local Security Manager，即面向独立部署的嵌入式管理软件。
  ✍ CLI-Command Line Interface，即面向专业用户的命令行管理工具。
- 多重高可靠性打造 99.999% 安全网络：多重高可靠(Multi-Layer High Availability，MLHA)是 TippingPoint IPS 为保证网络与业务的永续性而开发的专利技术，该技术面向业务传送的所有层面进行高可靠保护，使得在任何情况下业务都不会因为 IPS 的故障而中断。物理级保护和掉电事故保护、系统软件故障保护、冗余网络部署中的基于状态的业务保护、不间断的管理保护、SMS 提供的增强模式及 SMS 支持冗余部署等高可靠性的设计与协同工作，使得 TippingPoint IPS 系统成为 99.999% 电信级安全网络的坚强基石。

6.7 防火墙、IDS 与 IPS 比较

从 2003 年 Gartner 公司副总裁 Richard Stiennon 发表《入侵检测已寿终正寝，入侵防御将万古长青》的报告引发安全业界震动至今，关于入侵检测系统(IDS)与入侵防御系



统(IPS)之间关系的讨论已经趋于平淡。2006年互联网数据中心(Internet Data Center, IDC)年度安全市场报告更是明确指出IDS和IPS是两个独立的市场,给这场讨论画上了一个句号。

6.7.1 如何区分和选择IDS与IPS

目前无论是信息安全专业人士还是普通用户,都认为IDS和IPS是两类产品,并不存在IPS要替代IDS的可能。但IPS的出现的确给用户带来了新的困惑,有些用户进行产品选择时在产品类型上写着"入侵检测系统或者入侵防御系统"。其实从产品价值和应用角度来分析,可以很清晰地区分和选择IDS和IPS。

(1) 从产品价值角度来看,IDS注重的是网络安全状况的监管。用户进行网络安全建设之前,通常要考虑信息系统面临哪些威胁、威胁的来源以及进入信息系统的途径、信息系统对这些威胁的抵御能力等方面的信息。在信息系统建设中和实施后也要不断地观察信息系统中的安全状况,从而有的放矢地进行系统建设,根据安全状况及时调整安全策略,减少信息系统被破坏的可能。

IPS关注的是对入侵行为的控制。当用户明确信息系统安全建设方案和策略之后,可以在IPS中实施边界防护安全策略。与防火墙类产品可以实施的安全策略不同,IPS可以实施深层防御安全策略,即可以在应用层检测出攻击并予以阻断,这是防火墙所做不到的,当然也是IDS所做不到的。

(2) 从产品应用角度来看,为了达到可以全面检测网络安全状况的目的,IDS需要部署在网络内部的中心点,需要观察到所有网络数据。如果信息系统中包含了多个逻辑隔离的子网,则需要在整个信息系统中实施分布部署,以达到掌控整个信息系统安全状况的目的。

为了实现对外部攻击的防御,IPS需要部署在网络的边界。所有来自外部的数据必须串行通过IPS,IPS通过实时分析网络数据,发现攻击行为立即予以阻断,保证来自外部的攻击数据不能通过网络边界进入网络。

(3) 如何选择IDS和IPS。明确了上述区别,用户就可以比较理性地进行产品的类型选择。

- 若用户计划在一次项目中实施较为完整的安全解决方案,则应同时选择和部署IDS和IPS两类产品,在全网部署IDS,在网络的边界点部署IPS。
- 若用户计划分步实施安全解决方案,可以考虑先部署IDS进行网络安全状况监控,后期再部署IPS。
- 若用户仅仅关注网络安全状况的监控(如金融监管部门、电信监管部门等),只需在目标信息系统中部署IDS即可。

分析哪个产品更加满足用户需求,需要我们真正看清用户的安全需求到底是什么。很显然,用户需要的不是单一的产品,也不是众多产品的简单堆砌。现在一个比较流行的说法就是"信息安全保障体系(系统)",也就是用户的安全是要靠众多技术产品、服务和管理等要素组合成一个完整的体系,来解决所面临的安全威胁保护自己的信息资产和业务。

6.7.2　IPS 等于"防火墙＋IDS"吗

防火墙和 IDS 是两种截然不同的技术行为。

- 防火墙是网关形式，要求高性能和高可靠性。因此防火墙会非常看重吞吐率、延时、HA 等方面的要求。防火墙最主要的特征应当是通（传输）和断（阻隔）两个功能，所以其传输要求是非常高的。
- IDS 是一个检测和发现为特征的技术行为，其追求的是漏报率和误报率的降低。其对于性能的追求主要是在抓包不能漏，分析不能错，而不是微秒级的快速结果。IDS 由于其技术特征，所以其计算复杂度是非常高的。

IPS 试图将防火墙和 IDS 两个技术之间存在的天然矛盾糅合在一起，这在技术本质上存在的矛盾是客观的。

- 对于串接在网络中的 IPS 来说，分析得越清晰准确，计算复杂度越高，传输延迟就会大大增加。怎么能够让 IPS 去检测优秀 IDS 的超过 2000 多种攻击方法，而还能保持高的传输性能？
- IDS 的检测准确度是永远不能达到 100％，而防火墙的动作是一个绝对的阻断操作，用一个并不完全准确的检测结果，指导一个绝对的阻断操作，这个风险太大了。

因此，把 IPS 看做是防火墙和 IDS 的组合是不可能的。

6.7.3　检测和访问控制（防御）的协同是必然趋势

前面谈到检测技术和访问控制技术的矛盾，但是两个技术的协同工作和在应用上的融合又是一个迫切的要求和必然趋势。中国信息产业商会屈延文教授在《软件行为学》中提出"监测要集中，控制要分布"，这个观点对于如何看待检测类技术的走向是非常重要的。

一个准确度不能完全令人满意的 IDS，经过人工的分析可以变得准确；同样，经过大规模的 IDS 部署后的集中分析，以及和其他检测类技术的关联分析，可以获得更加精确的结果。这样的局部事件（Event）检测向全局性的事件（Incident）检测发展，根据全局性的检测结果就可以进行全局性的响应和控制。这是从宏观看检测和访问控制的融合方向。

全局性的检测可以有效提高检测的准确率，但是导致检测过程变长，局部速度不够快。因此，面对一些局部事件，针对其检测可以比较快速且阻断后带来的负面影响相对较小时，采用 IPS 将是一个较好的方案。

根据现有的检测、传输和芯片技术，目前 IPS 能够解决的主要是单包检测和高速传输的融合，对于端口扫描、拒绝服务、蠕虫等特征比较明确的攻击可以做到高效的检测和及时的阻断防护，而对于更为复杂的攻击（如采用变形攻击、攻击包拆分发送）则难以防范。

IDS 和 IPS 满足的是用户不同的安全需求。两种技术在相当长的时间里将与防火墙技术共存，在用户的信息安全保障体系中担当不同的角色，并协同工作。



6.8 习　　题

1. 入侵检测的作用是什么？入侵检测系统与防火墙有什么区别？
2. 请简单介绍入侵检测系统的通用模型。
3. 入侵检测的原理是什么？常用的入侵检测技术有哪些？
4. 入侵检测的流程包括哪些步骤？
5. 入侵检测系统可以分为哪几类？
6. 萨客嘶入侵检测系统有哪些功能？
7. Snort 有哪几种工作模式？其作用是什么？
8. 安装和配置 Snort 需要经过哪些步骤？
9. 入侵防御的原理是什么？
10. 入侵防御系统可以分为哪几类？
11. 简述防火墙、IDS 与 IPS 之间的关系。



第7章　网络安全隔离

本章学习目标：

- 理解网络安全隔离的意义。
- 掌握划分子网的方法。
- 掌握通过创建 VLAN 实现网络安全隔离的方法。
- 了解物理隔离产品及应用。

随着政府上网、企业上网、电子商务等一系列网络应用的蓬勃发展，Internet 正在逐渐融入社会的各个方面。一方面，网络用户成分越来越多样化，出于各种目的的网络入侵和攻击越来越频繁；另一方面，网络应用越来越深地渗透到金融、商务、国防等关键要害领域。换言之，Internet 网的安全，包括其中的信息数据安全和网络设备服务的运行安全，日益成为与国家、政府、企业的利益休戚相关的事情。

随着网络技术的发展，可以根据有特殊要求的部门和用户进行隔离保护，当然这里的隔离保护只是阻止未经允许的用户访问敏感部门和关键用户网络，而这些敏感部门和关键用户，可以通过相应配置与其他未被隔离的网络进行正常的数据交换，现在有如下三种解决方案。

(1) 通过子网掩码划分子网对网络进行隔离。这种方法可以充分、合理地利用 IP 地址资源，减少网络风暴，便于安全隔离管理，管理成本是最低的。

(2) 通过划分 VLAN 网段对网络进行隔离。这是对相关部门和用户在网络应用上进行功能细分，是一种软硬件的集合，普及性及适用性比较强。

(3) 通过构建网络隔离系统对网络进行隔离。这是对于有较高要求的网络应用。

本章着重介绍子网掩码划分、VLAN 虚拟网配置，物理隔离则通过具体产品及应用向大家介绍。

7.1　利用子网掩码划分子网的应用

7.1.1　Packet Tracer 模拟器简介

Packet Tracer 是由 Cisco 公司发布的一个辅助学习工具，为学习思科网络课程的初学者去设计、配置、排除网络故障提供了网络模拟环境。用户可以在软件的图形用户界面上直接使用拖曳方法建立网络拓扑，并可提供数据包在网络中行进的详细处理过程，观察网络实时运行情况。Packet Tracer 模拟器的主界面如图 7-1 所示。



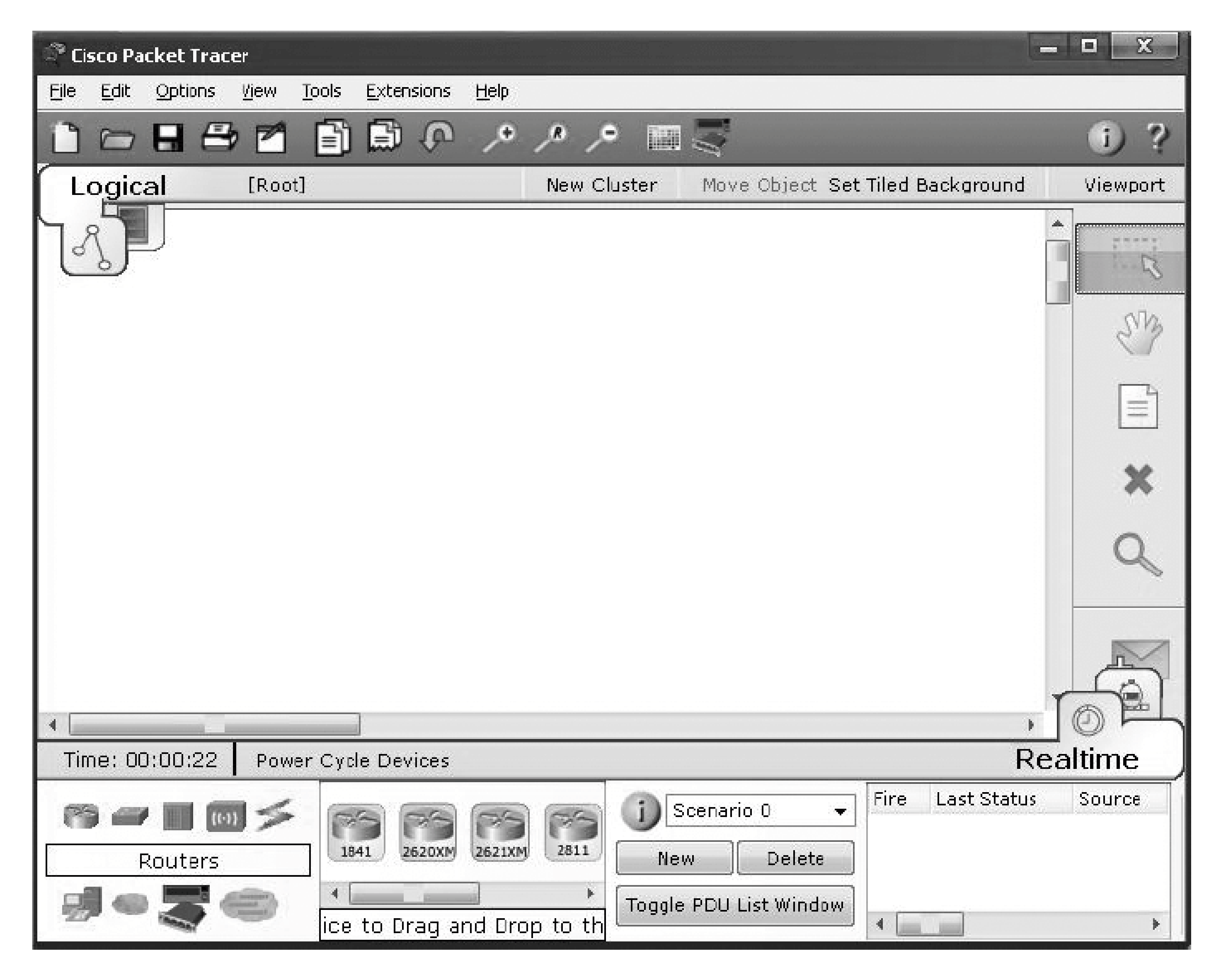


图 7-1 Packet Tracer 模拟器主界面

下面的项目设计可以在 Packet Tracer 模拟器中进行，其配置方法与真实设备配置方法相同。

7.1.2 项目背景及方案设计

1. 项目背景

某公司申请到 198.16.1.0/24 网段，设置了生产车间、销售处和财务处三个部门，各部门分处不同的地理位置。该公司需要建立内部网络，要求如下：

(1) 最大的部门可以容纳 30 台计算机。

(2) 各部门内部计算机终端之间能够直接通信。

(3) 各部门之间数据信息具有一定的独立性。

(4) 财务处的数据必须受到严格保护，非授权人员不能访问。

(5) 公司内所有计算机都能够访问互联网。

(6) 网络设备要高速、稳定运行。

2. 方案设计

根据公司要求，设计方案如下。

(1) 通过子网掩码划分子网，使三个部门分别属于不同的子网，便于管理。

(2) 各部门分别配置一台交换机，用于连接该部门所有终端设备。

(3) 各部门之间通过路由器连接，实现互相通信，并通过该路由器连接到 Internet。

(4) 方案的网络拓扑图如图 7-2 所示。

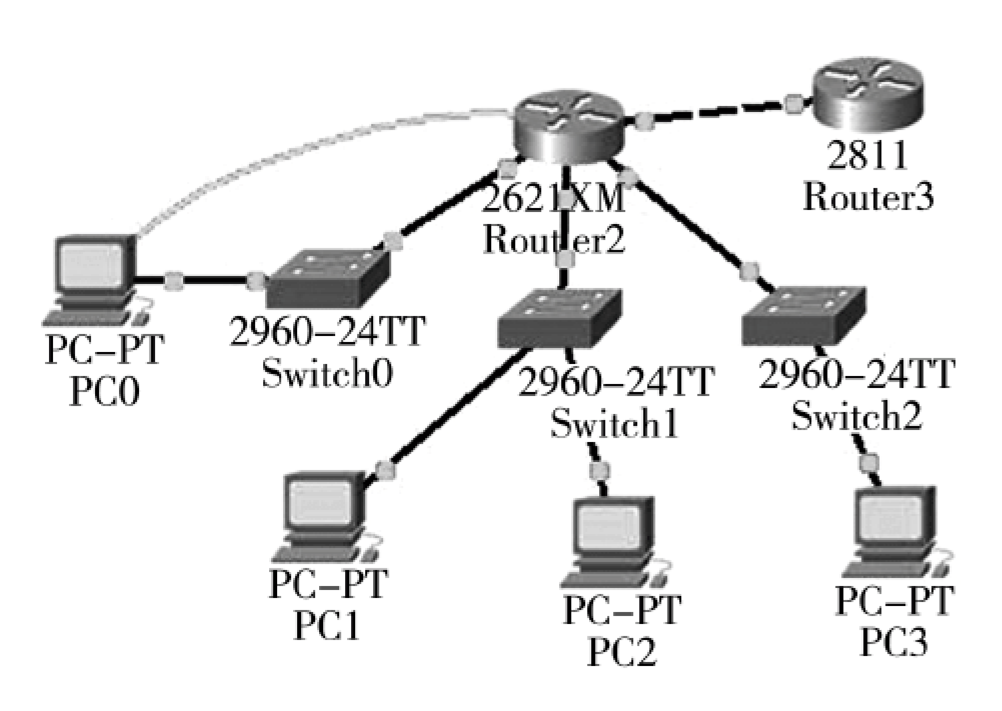


图 7-2 子网掩码划分子网网络拓扑图



（5）路由器 Router2 端口规划如表 7-1 所示。

表 7-1　路由器 Router2 端口规划

设备名称	端口	用途
Router2	FastEthernet 0/0	连接 Switch0
	FastEthernet 0/1	连接 Switch1
	FastEthernet 1/0	连接 Switch2
	FastEthernet 1/1	连接远程分支机构

7.1.3　实施步骤

实现子网掩码划分子网的步骤如下。

1. 确定子网掩码

根据公司原申请到的 198.16.1.0/24 网段，可知其原子网掩码为：255.255.255.0。现在需要划分子网，即考虑从原子网掩码的第四字节（主机位）中画出最高的几位作网络位，用于划分子网。

（1）假设子网的主机位位数。由于最大的部门有 30 台计算机，由下面的推算可知，子网的主机位位数至少为 5 位。

$$2^5 - 2 = 30$$

（2）确定子网的网络位数。由第二步可假设子网的主机位位数为 5 位，则子网的网络位位数为 3 位，由下面的计算可知，3 位网络位可以划分为 6 个子网，而公司有三个部门，完全满足要求。

$$2^3 - 2 = 6$$

注意：减 2 的原因：划分子网通常不采用子网号全为 0 或全为 1 的子网。子网号全为 0 时，与划分子网前的原网络号相同，不便于区分是子网络还是原网络。子网号全为 1 时，其广播地址与原网络的广播地址相同，不便于区分。因此，划分子网后得到的实际子网数应减 2，才得到可用子网数。

（3）确定子网掩码。根据上述步骤，确定子网的网络位位数为 3、主机位位数为 5。于是可以由下面的计算得到子网掩码为 255.255.255.224。

$$(11100000)_2 = (224)_{10}$$

2. 确定并分配子网及 IP 地址范围

（1）确定子网及 IP 地址范围。进行子网划分后，即可确定各子网的网络号及其 IP 地址范围等（如表 7-2 所示）。其中要排除子网号全为 0 和全为 1 的子网。



表 7-2　子网与相应 IP 地址范围

子　网　号	IP 地址范围
198.16.1.0(排除)	198.16.1.1 ～ 198.16.1.30
198.16.1.32	198.16.1.33 ～ 198.16.1.62
198.16.1.64	198.16.1.65 ～ 198.16.1.94
198.16.1.96	198.16.1.96 ～ 198.16.1.126
198.16.1.128	198.16.1.129 ～ 198.16.1.158
198.16.1.160	198.16.1.161 ～ 198.16.1.191
198.16.1.192	198.16.1.193 ～ 198.16.1.222
198.16.1.224 (排除)	198.16.1.225 ～ 198.16.1.254

(2) 分配子网并设置默认网关。可以在表 7-2 中的 6 个可用子网中任选 3 个子网分配给公司的三个部门,然后给三个部门的 PC 分配 IP 地址、子网掩码和默认网关。例如,如表 7-3 所示给三个部门分配子网,并设置默认网关。

表 7-3　子网及 IP 地址分配

部门名称	子　网　号	默认网关	示例 PC
生产车间	198.16.1.32	198.16.1.33	PC0
销售处	198.16.1.64	198.16.1.65	PC1、PC2
财务处	198.16.1.96	198.16.1.97	PC3

3. 搭建如图 7-4 所示网络环境,配置 Router2 路由器

使用 Console 控制台电缆将路由器 Router2 的控制台端口(Console 端口)与 PC0 的 COM1 或 COM2 串行接口相连。在 PC0 上选择【开始】/【程序】/【附件】/【通信】/【超级终端】命令,配置并运行超级终端程序。连接路由器,开始路由器的加电启动。然后登录路由器,进行路由器的配置。步骤如下:

(1) 当用户登录路由器时,所处的命令执行模式为用户 EXEC 模式,在此模式下执行 enable 命令进入特权 EXEC 模式。

```
Router>enable
```

(2) 在特权模式下,执行 Configure terminal 命令进入全局配置模式。

```
Router#Configure terminal
```

(3) 设置控制台的用户级登录密码和进入特权模式的密码。

根据公司需求,财务处的数据必须受到严格保护,非授权人员不能访问。因此,对路由器设置控制台的用户级登录密码和进入特权模式的密码。

① 设置控制台的用户级登录密码为 cisco

```
Router(config)#line console 0
```



```
Router(config-line)#password cisco
! 使所设置的密码起效
Router(config-line)#login
Router(config-line)#exit
```

② 设置进入特权模式的密码为 ciscoen

```
Router(config)#enable passwore ciscoen
或者 SWA(config)#enable secret ciscoen
```

其中，enable secret 命令设置的密码在配置文件中是加密保存的，强烈推荐采用该方式；而 enable passwore 命令所设置的密码在配置文件中采用明文保存。

(4) 选择 f0/0 端口，启用该端口。

```
Router(config)#int f0/0
Router(config-if)#no shutdown
```

(5) 配置该端口的 IP 地址。

```
Router(config-if)#ip address 198.16.1.33 255.255.255.224
```

(6) 退出到上一级模式。

```
Router(config-if)#exit
```

(7) 配置连接其他交换机的 f0/1 端口和 f1/0 端口。

```
Router(config)#int f0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 198.16.1.65 255.255.255.224
Router(config-if)#exit
Router(config)#int f1/0
Router(config-if)#no shutdown
Router(config-if)#ip address 198.16.1.97 255.255.255.224
Router(config-if)#exit
Router(config)#int f1/1
Router(config-if)#no shutdown
Router(config-if)#ip address 10.1.1.10 255.255.255.0
```

(8) 执行 end 命令可以直接退回到特权模式。

```
Router(config-if)#end
```

(9) 保存配置。

配置完毕后，必须退到特权模式下，使用 write 命令保存。否则，路由器断电重启后，所作的配置修改无效。

```
Router#write
```

代表远程机构的路由器 Router3 的配置，只需启用其与 Router2 连接的端口即可。

4. 配置各 PC

根据表 7-2 中示例 PC 所属地址空间，配置各 PC 的 IP 地址、子网掩码和默认网关。



5. 测试子网之间的连通性

(1) 测试不同子网间的连通性。在任意两台不同子网的 PC 之间使用 Ping 命令，测试子网之间的连通性，如果连通则说明配置正确：各部门之间通过子网掩码划分子网实现了相互通信。

(2) 测试各 PC 与 Router2 的 f0/1 端口的连通性。在各 PC 上使用 Ping 命令测试与 R0 路由器 f0/1 端口(IP 地址：10.1.1.10/24)的连通性，可以连通则说明网络配置正确，公司内所有计算机都可以访问互联网。

7.2 VLAN 子网的划分

除了通过子网掩码来划分网络外，目前网络中还有另外一种网络的划分，那就是 VLAN。

7.2.1 VLAN 简介

VLAN(Virtual Local Area Network，虚拟局域网)是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组的新兴技术。

IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 802.1Q 协议标准草案。VLAN 是为解决以太网的广播问题和安全性提出的，它在以太网帧的基础上增加了 VLAN 头，用 VLAN ID 把用户划分为更小的工作组，限制不同工作组间的用户二层互访，每个工作组就是一个虚拟局域网。虚拟局域网的好处是可以限制广播范围，并能够形成虚拟工作组，动态管理网络。

7.2.2 VLAN 的划分

VLAN 技术允许网络管理者将一个物理的 LAN 逻辑地划分成不同的广播域，每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。但由于它是逻辑地而不是物理地划分，所以同一个 VLAN 内的各个工作站无须被放置在同一个物理空间里，即这些工作站不一定属于同一个物理 LAN 网段。一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，即使是两台计算机有着同样的网段，但是它们却没有相同的 VLAN 号，它们各自的广播流也不会相互转发，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

VLAN 大致可以划分为如下四类。

1. 根据端口来划分 VLAN

这种划分方式是将交换机的端口分别划分到不同的 VLAN 中，从而形成多个 VLAN 子网。例如，将一台交换机的 1～5 号端口划分到 VLAN 10，将 6～10 号端口划分到 VLAN 20。同一个 VLAN 中的计算机属于同一个网段，可以直接通信，而不同 VLAN 之间的通信需要通过路由器或三层交换机进行。

第二代端口 VLAN 技术允许跨越多台交换机的多个不同端口划分 VLAN，不同交换机上的若干个端口可以组成同一个虚拟网。

以交换机端口来划分网络成员，其配置过程简单明了。因此，从目前来看，这种根据端口来划分 VLAN 的方式仍然是最常用的一种方式。

2．根据 MAC 地址划分 VLAN

这种划分 VLAN 的方法是根据每个主机的 MAC(Media Access Control，介质访问控制)地址来划分，即对每个 MAC 地址的主机都配置它属于哪个组。这种划分 VLAN 方法的最大优点就是当用户物理位置移动时，即从一台交换机换到其他的交换机时，VLAN 不用重新配置，所以可以认为这种根据 MAC 地址的划分方法是基于用户的 VLAN，这种方法的缺点是初始化时，所有的用户都必须进行配置，如果有几百个甚至上千个用户的话，配置是非常累的。而且这种划分的方法也导致了交换机执行效率的降低，因为在每一台交换机的端口都可能存在很多个 VLAN 组的成员，这样就无法限制广播包了。另外，对于使用笔记本电脑的用户来说，他们的网卡可能经常更换，这样，VLAN 就必须不停地配置。

注意：MAC 地址是识别局域网中节点的标识。网卡的 MAC 地址是由网卡生产厂商烧入网卡的 EPROM(可擦写可编程只读存储器)，它存储了主机的地址，一般也是全球唯一的。地址一般由 6 组数字、字母组成，比如 00-50-BA-CE-07-0C。

3．根据网络层划分 VLAN

这种划分 VLAN 的方法是根据每台主机的网络层地址或协议类型(如果支持多协议)划分的，虽然这种划分方法是根据网络地址，比如 IP 地址，但它不是路由，与网络层的路由毫无关系。

该方法的优点是用户的物理位置改变了，不需要重新配置所属的 VLAN，而且可以根据协议类型来划分 VLAN，这对网络管理者来说很重要，另外，这种方法不需要附加的帧标签来识别 VLAN，这样可以减少网络的通信量。

该方法的缺点是效率低，因为检查每一个数据包的网络层地址是需要消耗处理时间的(相对于前面两种方法)，一般的交换机芯片都可以自动检查网络上数据包的以太网帧头，但要让芯片能检查 IP 帧头，需要更高的技术，同时也更费时。当然，这与各个厂商的实现方法有关。

4．根据 IP 组播划分 VLAN

IP 组播实际上也是一种 VLAN 的定义，即认为一个组播组就是一个 VLAN，这种划分的方法将 VLAN 扩大到了广域网，因此，这种方法具有更大的灵活性，而且也很容易通过路由器进行扩展，当然这种方法不适合局域网，主要是效率不高。

7.2.3　VLAN 的主要用途

在企业网络刚刚兴起之时，由于企业网络规模小、应用范围的局限性、对 Internet 接入的认识程度、网络安全及管理的贫乏等原因，使得企业网仅仅限于交换模式的状态。当工作



站的数量较多、信息流很大的时候，就容易形成广播风暴，甚者造成网络瘫痪。

在采用交换技术的网络模式中，对于网络结构的划分采用的仅仅是物理网段的划分的手段。这样的网络结构从效率和安全性的角度来考虑都是有所欠缺的，而且在很大程度上限制了网络的灵活性。VLAN 对于一个规模较大的企业的网络应用，具有对不同职能部门的管理、安全和整体网络的稳定运行的优点。

使用 VLAN 具有以下优点。

1. 控制广播风暴

一个 VLAN 就是一个逻辑广播域，通过对 VLAN 的创建，隔离了广播，缩小了广播范围，可以控制广播风暴的产生。

2. 提高网络的安全性

由于不同 VLAN 间不可以直接通信，要实现通信必须通过具有网络层交换功能的路由器或第三层交换机。采用 VLAN 提供的安全机制，可以限制特定用户的访问，甚至锁定网络成员的 MAC 地址，从而限制了未经许可的用户对网络的访问，所以在一定程度上提高了网络的安全性。

3. 网络管理简单、直观

对于交换式以太网，如果对某些用户重新进行网段分配，需要网络管理员对网络系统的物理结构重新进行调整，甚至需要追加网络设备，增大网络管理的工作量。而对于采用 VLAN 技术的网络来说，一个 VLAN 可以根据部门职能、对象组或者应用将不同地理位置的网络用户划分为一个逻辑网段。在不改动网络物理连接的情况下可以任意地将工作站在工作组或子网之间移动。利用虚拟网络技术，大大减轻了网络管理和维护工作的负担，降低了网络维护费用。在一个交换网络中，VLAN 提供了网段和机构的弹性组合机制。

7.3 单一交换机 VLAN 的配置

在一台交换机上进行 VLAN 的划分及配置，是通过划分 VLAN 网段对网络进行隔离的最简单、最基本的形式。

搭建如图 7-3 所示网络环境，PC0、PC1 和 PC2 三台计算机分别连接到交换机的 1 号、6 号和 15 号端口。使用 Console 控制台电缆将交换机的控制台端口（Console 端口）与 PC0 的 COM1 或 COM2 串行接口相连。

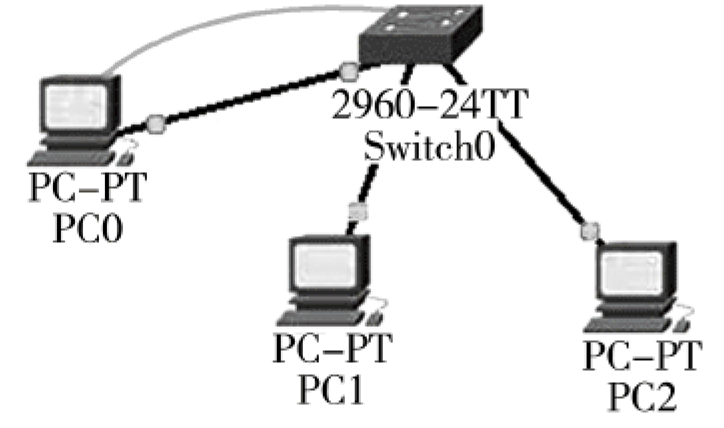


图 7-3　网络拓扑图

在 PC0 上选择【开始】/【程序】/【附件】/【通信】/【超级终端】命令，配置并运行超级终端程序。连接交换机，开始交换机的加电启动。然后登录交换机，就可以进行交换机的配置了。详细步骤如下。

1. 给交换机命名并设置登录密码

为了管理的方便，可以给交换机起名字。为了保障安全性，可以设置交换机控制台的用



户级登录密码和进入特权模式的密码。

(1) 当用户登录交换机时，所处的命令执行模式为用户 EXEC 模式，在此模式下执行 enable 命令进入特权 EXEC 模式。

```
Switch>enable
```

(2) 在特权模式下，执行 Configure terminal 命令进入全局配置模式。

```
Switch#Configure terminal
```

(3) 给交换机起名字为 SWA。

```
Switch (config)#hostname SWA
```

(4) 设置交换机控制台的用户级登录密码和进入特权模式的密码。

① 设置控制台的用户级登录密码为 cisco

```
SWA (config)#line console 0
SWA (config-line)#password cisco
```

！使所设置的密码起效

```
SWA (config-line)#login
SWA (config-line)#exit
```

② 设置进入特权模式的密码为 ciscoen

```
SWA (config)#enable passwore ciscoen
或者 SWA (config)#enable secret ciscoen
```

其中，enable secret 命令设置的密码在配置文件中是加密保存的，强烈推荐采用该方式；而 enable passwore 命令所设置的密码在配置文件中采用明文保存。

2. 显示 VLAN 配置信息

回到特权模式下执行 show vlan 命令，可以查看交换机的 VLAN 配置信息(图 7-4)。

```
SWA #show vlan
```

```
SWA#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    fa0/1, fa0/2, fa0/3, fa0/4
                                                fa0/5, fa0/6, fa0/7, fa0/8
                                                fa0/9, fa0/10, fa0/11, fa0/12
                                                fa0/13, fa0/14, fa0/15, fa0/16
                                                fa0/17, fa0/18, fa0/19, fa0/20
                                                fa0/21, fa0/22, fa0/23, fa0/24
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

图 7-4　显示输出的 VLAN 配置信息



默认情况下，交换机会自动创建和管理 VLAN 1，所有交换机端口默认属于 VLAN 1，用户不能删除该 VLAN。

提示：在这种配置下，网络中的任意两台 PC 都是互通的，可以使用 Ping 命令来验证这一点。

用户所创建的 VLAN 应从 2 开始，另外，交换机保留使用了 VLAN 1002～VLAN 1005 这四个 VLAN。最多可创建的 VLAN 数，受到交换机硬件条件限制，不同型号的交换机允许用户创建的 VLAN 数不同。

3. 创建 VLAN

(1) 进入数据库配置模式。

```
SWA# vlan database
```

(2) 为交换机创建 id 号为 2、5 的两个 VLAN，VLAN 的名字分别为 student 和 teacher。然后退出 VLAN 数据库配置模式。

```
SWA(vlan)#vlan 2 name student
SWA(vlan)#vlan 5 name teacher
SWA(vlan)#exit
```

4. 划分 VLAN 端口

VLAN 的创建可以在任意一台工作在 VTP Server 模式的交换机上进行，但要将端口划分给某个 VLAN，则必须在该端口所在的交换机上进行。要将一个端口设置为某个 VLAN 的成员，首先应选择该端口，然后在端口配置模式，通过以下命令实现。

例如，将 f0/1～f0/5、f0/15 六个端口分配到 VLAN 2，将 f0/6～f0/10 五个端口划分到 VLAN 5。配置步骤如下：

(1) 在特权模式下，执行 Configure terminal 命令进入全局配置模式。

```
SWA #configure terminal
```

(2) 执行 interface 命令进入端口配置模式，选择相关端口。

```
SWA (config)#interface range fa0/15
```

(3) 将端口设置为访问连接端口(大多数交换机的端口默认为访问连接端口)。

```
SWA (config-if)#switchport mode access
```

(4) 将端口划分到相应 VLAN 中，退回到上一级模式。

```
SWA (config-if)#switchport access vlan 2
SWA (config-if)#exit
```

(5) 通过使用 range 关键字，将一个端口范围划分到 VLAN。

```
SWA (config)#interface range fa0/1-5
SWA (config-if-range)#switchport mode access
```



```
SWA (config-if-range)#switchport access vlan 2
SWA (config-if-range)#exit
SWA (config)#interface range fa0/6-10
SWA (config-if-range)#switchport mode access
SWA (config-if-range)#switchport access vlan 5
```

（6）执行 end 命令可以直接退回到特权模式。

```
SWA (config-if-range)#end
```

（7）执行 show vlan 命令，可以看到输出的 VLAN 配置信息（图 7-5）。

```
SWA#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    fa0/11, fa0/12, fa0/13, fa0/14
                                                fa0/16, fa0/17, fa0/18, fa0/19
                                                fa0/20, fa0/21, fa0/22, fa0/23
                                                fa0/24, Gig1/1, Gig1/2
2    student                          active    fa0/1, fa0/2, fa0/3, fa0/4
                                                fa0/5, fa0/15
5    teacher                          active    fa0/6, fa0/7, fa0/8, Fa0/9
                                                fa0/10
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

图 7-5　创建 VLAN 后的 VLAN 配置信息

5. 保存配置

所有配置修改完毕后，必须退到特权模式下，使用 write 命令保存。否则，交换机断电重启后，所做的配置修改无效。

```
SWA #write
```

6. 测试

（1）测试 VLAN 内 PC 之间的连通性。PC0 和 PC2 都属于 VLAN 2，使用 Ping 命令可以看到它们是互通的（图 7-6）。

（2）测试 VLAN 间 PC 之间的连通性。PC0 与 PC1 属于不同的 VLAN，使用 Ping 命令可以看到它们是不连通的（图 7-7），说明通过使用 VLAN 实现了不同子网间的隔离（不同 VLAN 间的通信必须通过路由器或第三层交换机）。

```
PC>ping 192.168.2.102

Pinging 192.168.2.102 with 32 bytes of data:

Reply from 192.168.2.102: bytes=32 time=110ms TTL=128
Reply from 192.168.2.102: bytes=32 time=40ms TTL=128
Reply from 192.168.2.102: bytes=32 time=40ms TTL=128
Reply from 192.168.2.102: bytes=32 time=40ms TTL=128

Ping statistics for 192.168.2.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 110ms, Average = 57ms
```

图 7-6　Ping 成功的输出

```
PC>ping 192.168.5.101

Pinging 192.168.5.101 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.5.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

图 7-7　Ping 不成功的输出



注意：属于同一 VLAN 的 PC，其 IP 地址应设置为同一网段。如 PC0 的 IP 地址设为：192.168.2.100/24，PC2 的 IP 地址设为：192.168.2.102/24。而属于不同 VLAN 的 PC，其 IP 地址应设置为不同的网段，如 PC1 的 IP 地址设为：192.168.5.101/24。

7. 删除 VLAN

若要删除已创建的 VLAN，删除之前，必须先将属于该 VLAN 的端口删除（删除的端口自动划分回 VLAN 1 中），否则会出现端口消失的情况。如删除 VLAN 5，操作步骤如下。

（1）删除 VLAN 5 中的端口。

```
SWA (config)#interface range fa0/6-10
SWA (config-if-range)#no switchport access vlan 5
```

（2）退出端口配置模式，进入 VLAN 数据库管理模式。

```
SWA (config-if-range)#end
SWA#vlan database
```

（3）执行 no vlan 5 命令将 vlan 5 从数据库中删除。

```
SWA (vlan)#no vlan 5
```

（4）执行 exit 命令退出 VLAN 数据库配置模式，在特权模式下，执行 show vlan 命令可以看到 vlan 5 已被删除，端口 f0/6～f0/10 重新划分回 vlan 1 中（图 7-8）。

```
SWA#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    fa0/6, fa0/7, fa0/8, fa0/9
                                                fa0/10, fa0/11, fa0/12, fa0/13
                                                fa0/14, fa0/16, fa0/17, fa0/18
                                                fa0/19, fa0/20, fa0/21, fa0/22
                                                fa0/23, fa0/24, Gig1/1, Gig1/2
2    student                          active    fa0/1, fa0/2, fa0/3, fa0/4
                                                fa0/5, fa0/15
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

图 7-8　删除 VLAN 5 后的 VLAN 配置信息

7.4　跨交换机 VLAN 的配置

在多台交换机上进行 VLAN 的划分及配置，是通过划分 VLAN 网段对网络进行隔离的最常用、较复杂的形式。下面通过对一个具体项目的分析与设计来学习跨交换机 VLAN 的设计思路及配置。



7.4.1　VTP 简介

VTP(VLAN Trunking Protocol,VLAN 链路聚集协议)是一个在建立了汇聚链路的交换机之间同步和传递 VLAN 配置信息的协议,以在同一个 VTP 域中维持 VLAN 配置的一致性。在创建 VLAN 之前,应先定义 VTP 管理域。

1. VTP 工作模式

VTP 有 Server(服务器)、Client(客户端)和 Transparent(透明)三种工作模式。

(1) Server 模式下的交换机允许创建、修改和删除本地 VLAN 数据库中的 VLAN,允许设置一些对整个 VTP 域的配置参数。这些操作将传递到 VTP 域内所有处于 Server 或 Client 模式的其他交换机,以实现对 VLAN 信息的同步。

(2) Client 模式下的交换机不能创建、修改和删除 VLAN,主要通过 VTP 域内其他交换机的 VLAN 配置信息来同步和更新自己的 VLAN 配置。

(3) Transparent 模式下的交换机也允许创建、修改和删除本地 VLAN 数据库中的 VLAN,但与 Server 模式不同的是,对 VLAN 配置的变化,不会传播给其他交换机(仅对本机有效)。因此,工作于 Transparent 模式的交换机不需要事先创建 VTP 管理域。

2. 创建 VTP 管理域

(1) 创建 VTP 管理域。

① 在特权模式下,执行 vlan database 命令进入数据库配置模式。

```
Switch#vlan database
```

② 在数据库配置模式下,执行 vtp domain 命令创建名为 manager 的管理域。

```
Switch(vlan)#vtp domain manager
```

(2) 设置 VTP 模式。如设置 VTP 的工作模式为 Server。

```
Switch(vlan)#vtp server
```

(3) 执行 exit 命令退出 VLAN 数据库配置模式。

```
Switch(vlan)#exit
```

(4) 查看 VTP 信息。在特权模式下,执行 show vtp status 命令可以查看 VTP 的状态信息(图 7-9)。

```
Switch#show vtp status
```

VTP 管理域不仅可以在 VLAN 数据库中创建,也可以在全局配置模式下创建,在全局模式下创建的方法如下。

```
Switch#configure terminal
Switch(config)#vtp domain manager
```



```
Switch(config)#vtp mode server
Switch(config)#exit
```

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : manager
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xDE 0x28 0x72 0x50 0x9A 0x09 0xAA 0x7F
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

图 7-9　显示输出的 VTP 状态信息

7.4.2　项目背景及方案设计

1. 项目背景

某公司有计算机约 50 台，设置了信息处、销售处和财务处三个部门，各部门的地理位置如图 7-10 所示。该公司需要建立内部网络，要求如下：

(1) 各部门内部计算机终端之间能够直接通信。

(2) 各部门之间数据信息具有一定的独立性。

(3) 公司内所有计算机都能够访问互联网。

(4) 财务处的数据必须受到严格保护，非授权人员不能访问。

(5) 总经理兼管财务处，副总经理兼管销售处。

(6) 网络设备要高速、稳定运行。

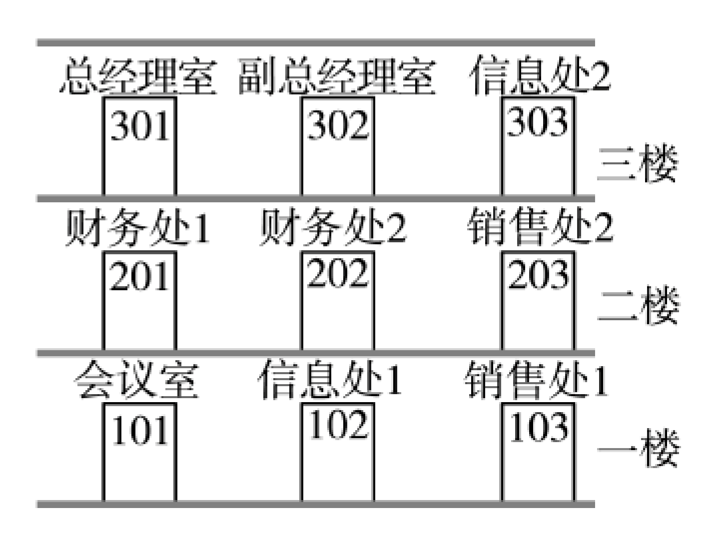


图 7-10　各部门地理位置

2. 方案设计

根据公司要求，设计方案如下。

(1) 每层楼配置一台交换机，用于连接该楼层所有终端设备。

(2) 创建 VTP 管理域，为每一个部门创建一个 VLAN。

(3) 在交换机上划分 VLAN，进行跨交换机 VLAN 的配置，实现各 VLAN 内部计算机终端能相互通信。

(4) 给各 VLAN 创建虚拟子端口 IP 地址，实现 VLAN 间的通信。

(5) 使用路由器连接到 Internet。

(6) 方案的网络拓扑图如图 7-11 所示。

(7) 各部门 IP 地址规划和各设备端口规划如表 7-4 和表 7-5 所示。



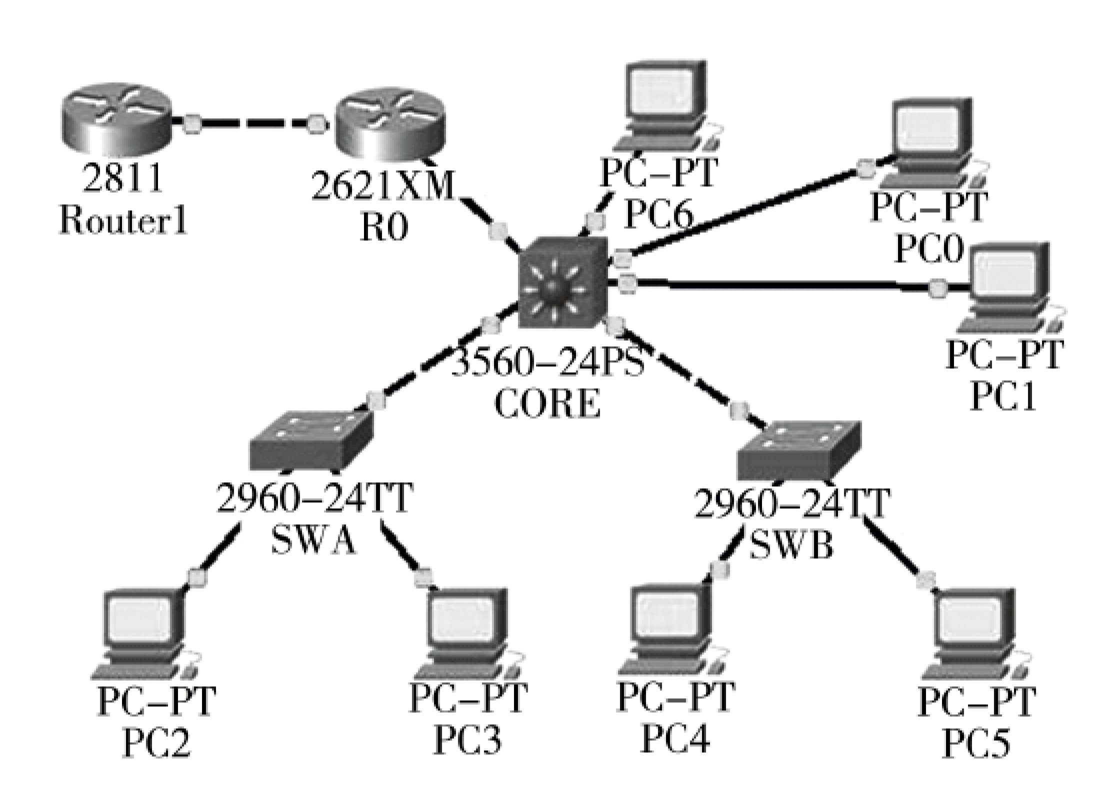


图 7-11　网络拓扑图

表 7-4　各部门 IP 地址规划

部门名称	地址空间	所属 VLAN	虚拟子端口 IP 地址（默认网关）	示例 PC 名称
总经理	192.168.5.100/24	VLAN 30	192.168.5.1/24	PC0
副总经理	192.168.3.101/24	VLAN 20	192.168.3.1/24	PC1
财务处	192.168.5.0/24	VLAN 30	192.168.5.1/24	PC4
信息处	192.168.2.0/24	VLAN 10	192.168.2.1/24	PC2、PC6
销售处	192.168.3.0/24	VLAN 20	192.168.3.1/24	PC3、PC5

表 7-5　各设备端口规划

设备名称	端口	用途	端口类型
R0	FastEthernet 0/0	连接 CORE	路由端口
	FastEthernet 0/1	连接远程分支机构	路由端口
CORE	FastEthernet 0/1-5	连接用户 PC	Access 端口，VLAN 10
	FastEthernet 0/11	连接总经理 PC	Access 端口，VLAN 30
	FastEthernet 0/12	连接副总经理 PC	Access 端口，VLAN 20
	FastEthernet 0/22	连接 SWB	Trunk 端口
	FastEthernet 0/23	连接 SWA	Trunk 端口
	FastEthernet 0/24	连接 R0	三层交换端口
SWA	FastEthernet 0/1-5	连接用户 PC	Access 端口，VLAN 10
	FastEthernet 0/6-10	连接用户 PC	Access 端口，VLAN 20
	FastEthernet 0/24	连接 CORE	Trunk 端口
SWB	FastEthernet 0/1-5	连接用户 PC	Access 端口，VLAN 30
	FastEthernet 0/6-10	连接用户 PC	Access 端口，VLAN 20
	FastEthernet 0/24	连接 CORE	Trunk 端口



7.4.3 VLAN 配置步骤

搭建如图 7-11 所示网络环境，实现跨交换机 VLAN 配置步骤如图 7-12 所示。下面详细介绍实现步骤。

1. 配置核心交换机

（1）创建 VTP 管理域。创建 VTP 管理域通常在核心交换机上进行，其工作模式设置为 Server。其他分支交换机通常配置为 Client 模式，它们从核心交换机中获取 VTP 信息。

因此，在 Cisco 3560 三层交换机（CORE）上创建 VTP 管理域，步骤如下：

① 设置三层交换机名字为 CORE。

```
Switch> enable
Switch# configure terminal
Switch(config)#hostname CORE
```

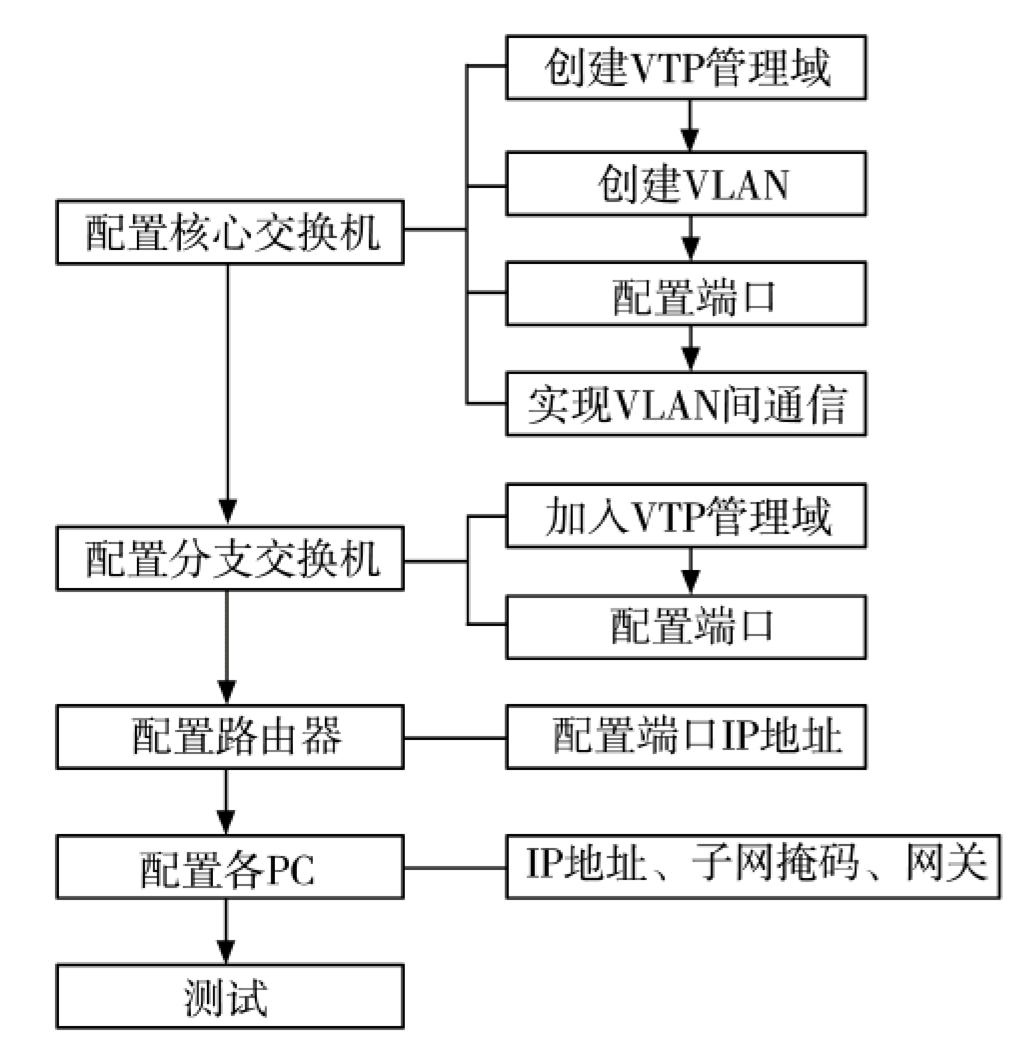


图 7-12　跨交换机 VLAN 配置步骤

② 设置控制台的用户级登录密码和进入特权模式的密码。根据公司需求，财务处的数据必须受到严格保护，非授权人员不能访问。因此，对交换机设置控制台的用户级登录密码和进入特权模式的密码。

- 设置控制台的用户级登录密码为 cisco。

```
CORE(config)#line console 0
CORE(config-line)#password cisco
CORE(config-line)#login
CORE(config-line)#exit
```

- 设置进入特权模式的密码为 ciscoen。

```
CORE(config)#enable secret ciscoen
```

③ 创建域名为 manager 的 VTP 管理域，其工作模式为 Server。

```
CORE(config)#vtp domain manager
CORE(config)#vtp mode server
CORE(config)#exit
```

（2）创建 VLAN。分别为信息处、销售处和财务处创建 VLAN，VLAN 的 id 号分别为 10、20 和 30，VLAN 名分别为 info、sale 和 fina。

```
CORE# vlan database
CORE(vlan)#vlan 10 name info
CORE(vlan)#vlan 20 name sale
CORE(vlan)#vlan 30 name fina
CORE(vlan)#exit
```



（3）配置端口

① 配置各 VLAN 端口。根据表 7-5 的端口规划，将相应端口划分到各 VLAN 中。

```
CORE# configure terminal
CORE(config)#int range f0/1-5
CORE(config-if-range)#switchport mode access
CORE(config-if-range)#switchport access vlan 10
CORE(config-if-range)#exit
CORE(config)#int f0/11
CORE(config-if)#switchport mode access
CORE(config-if)#switchport access vlan 30
CORE(config-if)#exit
CORE(config)#int f0/12
CORE(config-if)#switchport mode access
CORE(config-if)#switchport access vlan 20
CORE(config-if)#exit
```

② 配置其他端口。

- 配置 f0/24 为三层交换端口，其 IP 地址为：172.16.1.1/30，用于连接 R0 路由器。

```
CORE(config)#int f0/24
!设置为三层交换端口
CORE(config-if)#no switchport
!启用该端口
CORE(config-if)#no shutdown
CORE(config-if)#ip address 172.16.1.1 255.255.255.252
CORE(config-if)#exit
```

- 配置 f0/22 端口和 f0/23 端口为 Trunk 端口，用于连接分支交换机。

```
CORE(config)#int f0/22-23
!设置所选端口为 Trunk 端口
CORE(config-if)#switchport mode trunk
CORE(config-if)#exit
```

（4）实现 VLAN 间通信。VLAN 间要实现相互通信，必须在三层交换机上为每一个 VLAN 创建一个虚拟子端口，并设置端口的 IP 地址，这样就可以实现虚拟子端口之间的路由，从而实现 VLAN 间的通信。

```
!选择 vlan
CORE(config)#int vlan 10
!配置端口的 IP 地址
CORE(config-if)#ip address 192.168.2.1 255.255.255.0
CORE(config-if)#exit
CORE(config)#int vlan 20
CORE(config-if)#ip address 192.168.3.1 255.255.255.0
CORE(config-if)#exit
CORE(config)#int vlan 30
CORE(config-if)#ip address 192.168.5.1 255.255.255.0
CORE(config-if)#end
CORE #write
```



2. 配置分支交换机

(1) 配置左边 Cisco 2960 交换机(SWA)

① 加入 VTP 管理域。

```
Switch>en
Switch# conf terminal
Switch(config)#hostname SWA
SWA(config)#exit
!加入 vtp 管理域
SWA(config)#vtp domain manager
!设置为 Client 模式
SWA(config)#vtp mode Client
```

② 配置端口。

```
SWA(config)#int range f0/1-5
SWA(config-if-range)#switchport mode access
SWA(config-if-range)#switchport access vlan 10
SWA(config-if-range)#exit
SWA(config)#int range f0/6-10
SWA(config-if-range)#switchport mode access
SWA(config-if-range)#switchport access vlan 20
SWA(config-if-range)#exit
SWA(config)#int f0/24
!配置为 Trunk 端口,用于连接核心交换机
SWB(config-if)#switchport mode Trunk
SWA(config-if)#end
SWA# write
```

(2) 配置右边 Cisco 2960 交换机(SWB)

① 加入 VTP 管理域。

```
Switch>en
Switch# conf terminal
Switch(config)#hostname SWB
SWB(config)#vtp domain manager
SWB(config)#vtp mode client
```

② 配置端口。

```
SWB (config)#int range f0/1-5
SWB (config-if-range)#switchport mode access
SWB (config-if-range)#switchport access vlan 30
SWB (config-if-range)#exit
SWB (config)#int range f0/6-10
SWB(config-if-range)#switchport mode access
SWB (config-if-range)#switchport access vlan 20
SWB (config-if-range)#exit
SWB (config)#int f0/24
SWB (config-if)#switchport mode Trunk
```



```
SWB (config-if)#end
SWB #write
```

3. 配置路由器

设置路由器的名字为 R0,f0/0 端口用于连接 Cisco 3560 交换机,其 IP 地址为:172.16.1.2/30,f0/1 端口用于连接 Internet。

```
Router>enable
Router# conf terminal
Router(config)#hostname R0
R0(config)#int f0/0
!启用端口
R0(config-if)#no shutdown
R0(config-if)#ip address 172.16.1.2 255.255.255.252
R0(config-if)#exit
R0(config)#int f0/1
R0(config-if)#no shutdown
R0(config-if)#ip address 10.1.1.10 255.255.255.0
R0(config-if)#end
R0# write
```

代表远程机构的路由器 Router1 的配置,只需启用其与 R0 连接的端口即可。

4. 配置各 PC 机

根据表 7-4 中示例 PC 所属地址空间,配置各 PC 的 IP 地址、子网掩码和默认网关。

5. 测试

(1) 测试 VLAN 内各 PC 之间的连通性。对属于同一 VLAN 内的各 PC,使用 Ping 命令来验证连通性。结果是可以连通。

(2) 测试 VLAN 间各主机之间的连通性。对属于不同 VLAN 之间的各 PC,使用 Ping 命令来验证连通性。可以连通则说明网络配置正确,即通过配置第三层交换机实现了 VLAN 间的通信。

注意: 路由器或第三层交换机可以控制 VLAN 间的通信,可以灵活配置不同的用户访问权限,只对确实需要的一方或双方开放访问权限,可以确保关键子网的安全。

(3) 测试各 PC 与 R0 的 f0/1 端口的连通性。在各 PC 上使用 Ping 命令测试与 R0 路由器 f0/1 端口(IP 地址:10.1.1.10/24)的连通性,可以连通则说明网络配置正确:公司内所有计算机都可以访问互联网。

7.5　网络隔离概述

网络隔离是一项网络安全技术,通过隔离可以消除来自可信网络之外的威胁,同时能完成网络之间数据的安全交换。网络隔离技术与其他网络安全技术不同,比如,防火墙的作用



是在保障网络间互通的前提下，尽可能安全；而网络隔离则是在确保安全的前提下，尽可能让网络之间互通。因此，网络隔离技术弥补了原有安全技术的不足，有自己独特的优势。

7.5.1 网络隔离技术

1. 理解网络隔离

网络中的"隔离"与人们常识中的"隔离"其含义是不同的，从常识中理解"网络隔离"会认为是将两个或两个以上的网络相互断开、不能通信，这样的网络是没有实用价值的。网络中的"隔离"并不是网络间完全断开，而是隔离不安全因素，使受保护的网络能安全地与外部网络通信。

网络隔离，主要是指把两个或两个以上可路由的网络(使用 TCP/IP 协议)通过不可路由的协议(如 IPX/SPX、NetBEUI)进行数据交换而达到隔离目的。由于其原理主要是采用了不同的协议，通常也叫协议隔离。

网络隔离是目前最好的网络安全技术，它消除了基于网络和基于协议的安全威胁。

2. 网络隔离技术分类

基于网络安全的隔离技术主要有以下三类。

(1) 物理隔离。物理隔离是通过采用软、硬件结合的方法，使内部网络与外部网络之间的设备、数据信息相对独立。

(2) 网络隔离。网络隔离主要指协议隔离，是利用协议转换的方法进行网络间的数据交换。

(3) 安全隔离。安全隔离主要指利用专门的设备实现网络间的数据交换仅仅在应用层完成。

3. 网络隔离技术发展阶段

网络隔离技术的发展经历了以下五个阶段。

(1) 完全的物理隔离。采用完全独立的设备、存储和线路来访问不同的网络。需要至少两套网络和系统(一套用于访问内部网络；另一套用于访问外部网络)，它们之间是完全的物理隔离。存在信息交流不方便和成本高的缺点。

(2) 硬件隔离卡隔离。在客户端增加一块硬件卡，客户端硬盘或其他存储设备首先连接到该卡，然后再转接到主板上，通过该卡能选择并控制客户端硬盘或其他存储设备，实现不同网络的连接。存在一定的不安全因素。

(3) 数据转播隔离。利用转播系统分时复制文件的途径来实现隔离。切换时间非常久，甚至需要手工完成，无实用价值。

(4) 空气开关隔离。通过使用单刀双掷开关，使得内外部网络分时访问临时缓存器来完成数据交换。

(5) 安全通道隔离。通过专用通信设备、专有安全协议和加密验证等安全机制高效地实现内外部网络的隔离和数据交换，彻底阻断了网络间的直接 TCP/IP 连接，对网间通信的双方实施身份认证、内容过滤、安全审计等安全防护，透明支持多种网络应用，成为当前隔离技术的发展方向。

7.5.2　网络隔离安全要素

无论采用哪种网络隔离方案，都必须满足如下安全要素。

1. 隔离产品自身有较高的安全性

网络隔离产品至少具备两套主机系统，一套用于控制外部网络；另一套用于控制内部网络，数据交换是通过不可路由的协议在两套主机系统之间进行。因此，来自外部网络的威胁无法到达内部网络，保障了内部网络的安全。

2. 确保网络包不能到达受保护网络

网络隔离的关键是确保网络包不能到达受保护的网络。无论在两个网络间采用什么转换方式，只要网络包能够进入受保护网络，就不能达到隔离的效果。即使将网络包转换为文本进行交换也不行。

3. 只允许应用层数据交换

为了消除大量来自网络层的攻击，必须对数据包进行协议分析，得到应用层数据，并以此数据进行网络间交换，提高受保护网络的安全性。

4. 在确保安全的前提下尽可能畅通

网络隔离产品往往部署在网络之间数据交换的关键点，对通信流量和速率有一定要求。因此，网络隔离产品应有较高的处理性能，不能成为网络交换的瓶颈；要有较强的适应性，能透明地接入网络，透明地支持多种应用。

7.6　物理隔离

物理隔离是指内部网络不得直接或间接地连接外部网络即互联网。物理隔离技术通过中断内部网络与外部网络的连接，不支持 TCP/IP 协议，不依赖于操作系统，解决了目前网络安全存在的根本性问题，即由于操作系统漏洞和 TCP/IP 协议漏洞所带来的安全问题，有效地防止了恶意代码、病毒以及网络入侵的发生，满足了网络安全的机密性、完整性、可用性、可控性和可审查性要求。

7.6.1　物理隔离原理

物理隔离设备在任意时刻只能与一个网络的主机系统建立非 TCP/IP 协议的数据连接，即当它与外部网络的主机系统连接时，它与内部网络的主机系统必须是断开的；反之亦然，保证内、外部网络不能同时连接在物理隔离设备上。

通过如下步骤对物理隔离原理进行说明。

（1）当内网与专网之间无信息交换时，物理隔离设备与内网之间、物理隔离设备与专用



网之间、内网与外网之间是完全断开的，如图 7-13 所示。

(2) 当外网有数据需要到达内网的时候，控制电路控制隔离设备与外网服务器建立非 TCP/IP 的数据连接，如图 7-14 所示。此时隔离设备将所接收的外网数据进行协议剥离。

(3) 一旦数据完全写入外网存储设备，隔离设备在控制电路的控制下立即中断与外网的连接，转而发起对内网的非 TCP/IP 协议的数据连接，如图 7-15所示。然后将存储在外网存储设备中的数据转发给内网存储设备。内网收到数据后，立即进行 TCP/IP 协议和其他应用协议的封装，并交给应用系统。

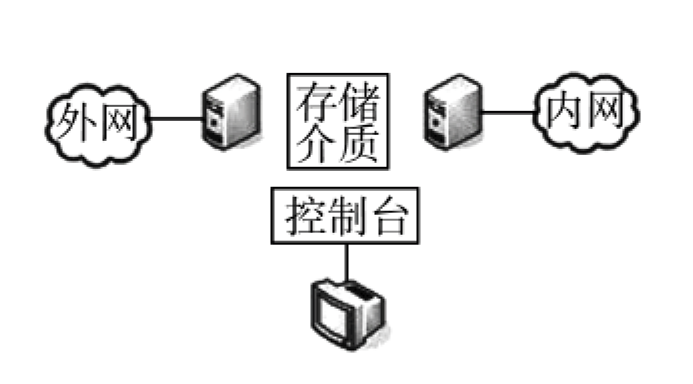


图 7-13　内外网没有通信请求时为断开状态

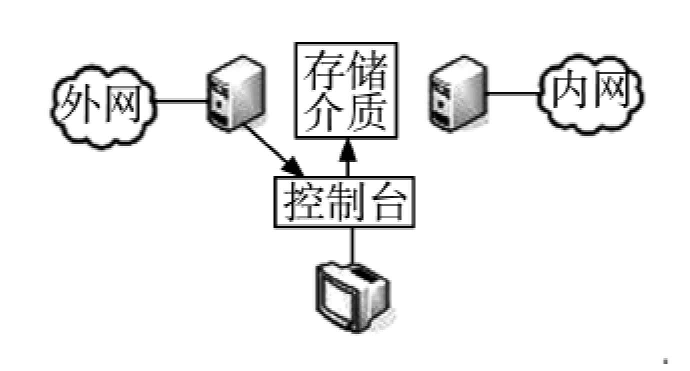


图 7-14　外网向内网发起非 TCP/IP 连接

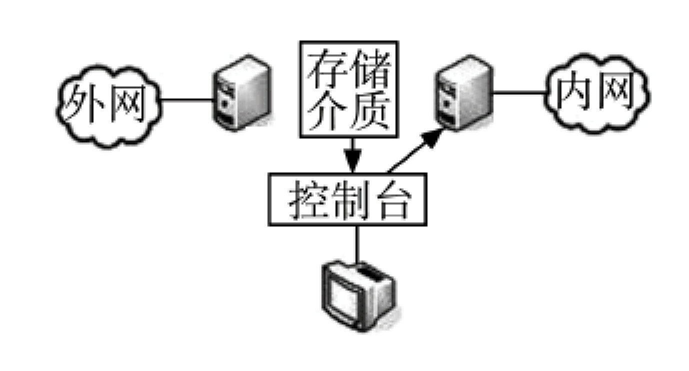


图 7-15　内网转发数据

(4) 在控制台收到完整的交换信号之后，控制电路控制隔离设备立即切断隔离设备与内网的连接，又回到如图 7-13 所示的内外网完全断开状态。这样就完成了外网向内网发送数据的全过程。

(5) 如果这时内网有文件需要发出，隔离设备在收到内网建立连接的请求之后，控制电路控制隔离设备建立与内网之间的非 TCP/IP 协议的数据连接，如图 7-16 所示。隔离设备剥离所有的 TCP/IP 协议和其他应用协议只接收原始的数据，将数据写入外网专用存储设备中。

(6) 当数据完全写入内网专用存储设备后，控制电路控制隔离设备立即中断与内网的连接，如图 7-17 所示。转而发起对外网的非 TCP/IP 协议的数据连接，内网存储设备中的数据转发到外网专用存储设备。外网收到数据后，立即进行 TCP/IP 的封装，并交给系统向外发送。

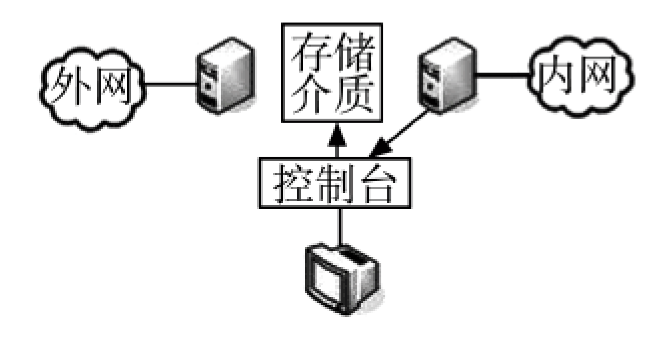


图 7-16　内网向外网发起非 TCP/IP 连接

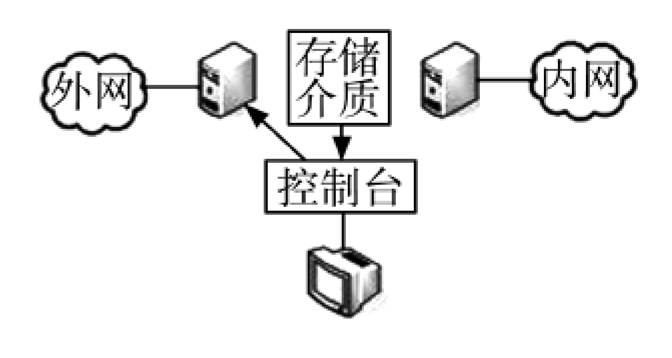


图 7-17　向外网转发数据

(7) 在所有的数据发送完成后，控制电路就会控制隔离设备立即中断隔离设备与外网的连接，恢复到如图 7-15 所示的完全隔离状态。这样就完成了一次完整的内网向外网发送数据的全过程。

每一次数据交换，隔离设备都经历数据的接收、存储和转发三个过程。物理隔离的一个特征就是内网与外网总是不连接的，内网和外网在同一时间最多只有一个与隔离设备建立非 TCP/IP 协议的数据连接。其数据传输机制是存储和转发。物理隔离的优点是明显的，即使外网在最坏的情况下，内网也不会受任何影响，修复外网系统也非常容易。

常见的物理隔离产品主要有物理隔离卡和物理隔离网闸，下面分别介绍。



7.6.2　物理隔离卡

1. 物理隔离卡

物理隔离卡是物理隔离的低级实现形式，一个物理隔离卡只能管一台个人计算机，甚至只可能在 Windows 环境下工作，每次切换都需要开关机一次。物理隔离网闸是物理隔离的高级实现形式，网闸可以管理整个网络，不需要开关机。网闸实现后，原则上不再需要物理隔离卡。安全隔离是一种逻辑隔离，防火墙就是一种逻辑隔离，因此防火墙也是一种安全隔离。有些厂商对安全隔离增加了一些特点，如采用了双主机结构，但双主机之间却是通过包来转发的。

2. 物理隔离卡产品：ZSD-32S 单硬盘物理隔离卡

ZSD-32S 单硬盘物理隔离卡系列是宙斯盾公司研制的拥有自主产权的新一代网络安全物理隔离产品(图 7-18)。隔离卡实现将一台计算机虚拟分成两台相对独立的计算机，硬盘安全部分连接内网，硬盘公共部分连接外网，通过内外网切换实现了物理隔离，确保内网信息安全和连接公共网络。外网接入满足专线、宽带、ADSL 等多种上网方式，采用启动界面选择、桌面切换软件等网络切换方式，方便使用。实现了单机到网络的隔离，在保证安全的基础上，用户可分时连接两套安全要求不同的网络。保护 CMOS 和 BIOS 信息不被篡改，从硬件上避免内网数据的安全隐患。实现了从内网到外网的身份认证，内外网实行不同权限的管理。


图 7-18　ZSD-32S 单硬盘物理隔离卡

7.6.3　物理隔离网闸

1. 物理隔离网闸

物理隔离网闸主要由内网处理单元、外网处理单元、安全隔离与信息交换处理单元三部分组成。外网处理单元与外网(如 Internet)相连，内网处理单元与内网(如军队网)相连；安全隔离与信息交换处理单元通过专用硬件断开内、外网的物理连接，并在任何时刻只与其中一个网络连接，读取等待发送的数据，然后“推送”到另一个网络上。在切换速度非常快的情况下，可以实现信息的实时交换。

2. 物理隔离网闸产品

常见的物理隔离产品有以下几种。

(1) 联想网御 SIS-3000 系列安全隔离网闸。联想网御 SIS-3000 系列安全隔离网闸作为网络链路层物理隔离设备(图 7-19)，具有比防火墙更高的安全性能。可在涉密网络之间、涉密网络不同安全域之间、涉密网络与内部网之间、内部网与互联网之间信任的进行信息交换。适用于政府、军队、金融等单位的网间非实时信息交换环境。



联想网御 SIS-3000 具有高速电子开关和专有协议，确保内外网在任意时刻物理隔离，通过领先的信息摆渡机制，提高数据传输的安全性；采用多种安全技术，支持可信的专用信息交换服务；使用高速安全隔离电子开关，支持毫秒级高速切换；自主的嵌入式安全操作系统，有效保证了系统自身安全性；支持包括文件交换、邮件交换和数据库同步在内的多种应用。

(2) 天行安全隔离网闸(Topwalk-GAP)。作为国内 GAP 领域的倡导者和领先者，天行安全隔离网闸(Topwalk-GAP)一直以其创新实用性、安全可靠性得到了广大用户的青睐(图 7-20)。



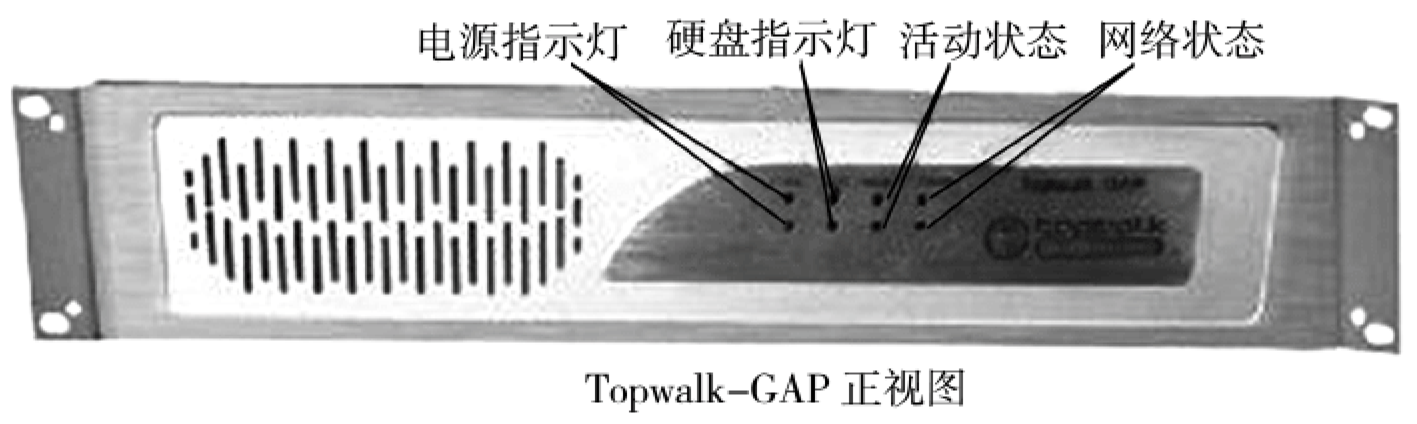
图 7-19　联想网御 SIS-3000



图 7-20　Topwalk-GAP

Topwalk-GAP 作为国内基于 GAP 技术的新一代安全隔离与信息交换产品，能够实现隔离网络间异构数据库交换。该产品的基本模块作为整个安全隔离网闸的核心部件，是其他应用模块的安全平台，数据库交换模块支持多种主流数据库平台在网络间的可控方向的安全数据交换，文件交换模块提供网络间的基于文件形式的可控方向的安全文件传输，消息模块为上层应用平台提供了基于 API 的开发接口，为彼此隔离的网络上层程序提供快速可靠的消息传送。

(3) 伟思安全隔离与信息交换系统。伟思安全隔离与信息交换系统(以下简称 ViGap)是伟思(集团)有限公司基于多年的物理隔离和网络安全技术的研究(图 7-21)，采用先进的反射 GAP 技术和协议终止技术独立研制的安全产品。ViGap 通过专用隔离硬件在可信网络与不可信网络间实现物理隔断，并通过基于硬件设计的反射 GAP 系统，实现在线高速实时的数据传输。



Topwalk-GAP 正视图

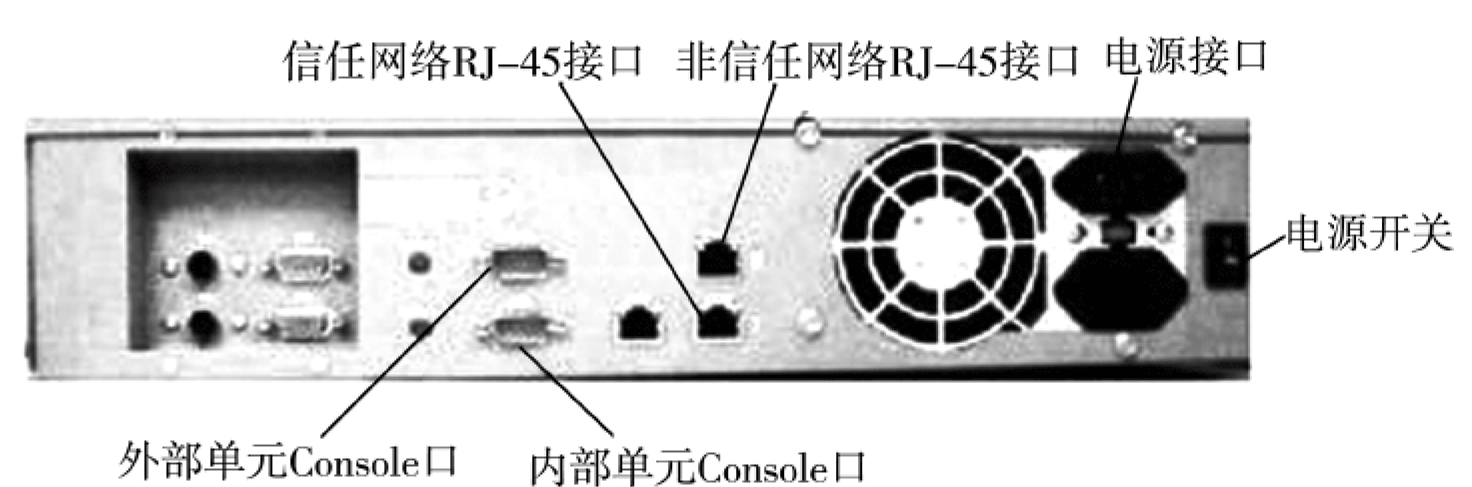


图 7-21　伟思安全隔离与信息交换系统(ViGap)

ViGap 系统由可信网络端处理系统、不可信网络端处理系统和反射 GAP 系统三部分系统组成，并具备强大的协议终止、协议检查、文本搜索、内容审查等功能，既能阻止网络层和操作系统层的各类已知攻击行为，又能防范未知攻击。



ViGap是以硬件隔离部件为基础的软硬件有机整合的网络安全产品。具有GAP技术必备的四个重要安全特性：硬件的物理隔离开关部件、协议的分拆和重组、细粒度的访问控制和日志管理和安全策略的灵活自定义。ViGap同时具备的三大技术优势是采用了先进的电子开关通断技术、反射Gap技术以及协议终止及分析技术。

(4) 中网物理隔离网闸。由中网公司研制开发的安全隔离和信息交换系统(X-Gap)，能够较好地解决隔离断开和数据交换的难题。X-Gap中断了两个网络之间的链路连接、通信连接、网络连接和应用连接，在保证两个网络完全断开和协议中止的情况下，以非网络方式实现了数据交换。没有任何包、命令和TCP/IP协议(包括UDP和ICMP)可以穿透X-Gap，它具有高安全、高带宽、高速度、高可用性的优点。此外，由于采用了SCSI技术，背板速率高达5G，开关效率达到纳秒级，彻底解决了速度慢、效率低的问题。除此之外，SCSI控制系统本身具有不可编程的特性和冲突机制，形成简单的开关原理，从而彻底解决了网闸开关的安全性问题。

3. 物理隔离网闸的应用

物理隔离网闸可应用于下面五种典型的场合。

(1) 局域网与互联网之间(内网与外网之间)。有些局域网络，特别是政府办公网络，涉及政府敏感信息，有时需要与互联网在物理上断开，用物理隔离网闸是一种常用的办法。

(2) 办公网与业务网之间。由于办公网与业务网的信息敏感程度不同，例如，银行的办公网和银行业务网就是很典型的信息敏感程度不同的两类网络。为了提高工作效率，办公网有时需要与业务网交换信息。为解决业务网的安全，比较好的办法就是在办公网与业务网之间使用物理隔离网闸，实现两类网络的物理隔离。

(3) 电子政务的内网与专网之间。在电子政务系统建设中要求政府内网与外网之间用逻辑隔离，在政府专网与内网之间用物理隔离。现常用的方法是用物理隔离网闸来实现。

(4) 业务网与互联网之间。电子商务网络一边连接着业务网服务器，一边通过互联网连接着广大民众。为了保障业务网服务器的安全，在业务网与互联网之间应实现物理隔离。

(5) 涉密网与非涉密网之间。电子政务建设中一般都对网络按照安全级别进行了安全域的划分，这在一定程度上保证了信息的安全，非涉密的系统及面向公众的信息采集和发布系统主要运行在非涉密网部分。涉密网、非涉密网之间物理隔离，依照涉密信息“最小化”原则，进行涉密网和非涉密网之间两个不同的信息安全域信息的适度“可靠交换”。

7.7　习　　题

1. 使用VLAN具有哪些优点?
2. 简述跨交换机的VLAN配置步骤。
3. 如何在中小企业网中规划与实施VLAN?
4. 简述网络隔离的含义。
5. 网络隔离的安全要素有哪些?
6. 简述物理隔离的原理。
7. 简述物理隔离网闸的主要应用。

第8章　PKI与加密技术

本章学习目标：

- 了解 PKI 技术及其应用。
- 了解数字证书及其作用。
- 了解密码技术的分类及其算法。
- 掌握 EFS 加密与解密的方法。
- 掌握 EFS 文件恢复代理的创建方法。
- 掌握密钥的存档与恢复方法。
- 掌握邮件的加密和数字签名方法。

随着网络技术的发展，特别是 Internet 的全球化，各种基于互联网技术的网上应用，如电子商务和电子政务、网上银行、网上证券和网上税务，以及企业或组织内部的信息安全管理等得到了迅猛发展。网络正逐步成为人们工作、生活中不可分割的一部分。由于互联网的开放性和通用性，网上的所有信息对所有人都是公开的，因此，应用系统对信息的安全性提出了更高的要求：需要验证身份的合法性；需要保证数据的保密性、完整性及传输的安全性；需要确保不可抵赖性。

公钥基础设施（Public Key Infrastructure，PKI）基于非对称公钥体制，采用数字证书（可简称为：证书）管理机制，可以透明地为网上应用提供上述安全服务，极大地保证了网上应用的安全性。

通常在企业或组织网络内部需要对一些重要的文件进行加密存放，利用 Windows Server 2003 家族的 PKI 技术，通过配置系统的 EFS（Encrypting File System，加密文件系统）和证书服务，可以实现对文件和文件夹的加密存储；当密钥意外丢失时还可以通过配置故障恢复代理恢复加密的文件。在互联网中，利用 PKI 技术可以实现对邮件的加密和数字签名，文件加密技术可以确保文件在传输途中的安全，而数字签名技术则可以确保文件是由正确的人发送的。

密码技术是信息交换安全的基础，本章将对对称密钥算法、非对称密钥算法和单向散列函数三类密码技术进行介绍。

8.1　PKI 技术及其应用

8.1.1　PKI 概述

PKI 产生于 20 世纪 80 年代，它是提供公钥加密和数字签名服务的系统或平台，目的是为了管理密钥和证书。PKI 采用数字证书进行公钥管理，通过第三方的可信任机构——证书颁发机构(Certificate Authority，CA)，把用户的公钥和用户的其他标识信息捆绑在一起(包括用户名和电子邮件地址等信息)，以便在互联网上验证用户的身份。PKI 把公钥密码和对称密码结合起来，在互联网上实现密钥的自动管理，保证网上数据的安全传输。

因此，从大的方面来说，所有提供公钥加密和数字签名服务的系统，都可归结为 PKI 系统的一部分，PKI 为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便地使用加密和数字签名技术，从而保证网上数据的机密性、完整性和有效性。

在 PKI 体系中，CA 和数字证书是密不可分的两个部分。CA 是负责产生、分配并管理数字证书的可信赖的第三方权威机构，是 PKI 安全体系的核心环节。CA 通常采用多层次的分级结构，上级认证中心负责签发和管理下级 CA 的证书，最下一级的 CA 直接面向最终用户。

8.1.2　数字证书及其作用

1. 数字证书

数字证书是一种权威性的电子文档，由 CA 发放并经 CA 数字签名，它提供了一种在互联网上验证用户身份的方式，其作用类似于司机的驾驶执照或日常生活中的身份证。

最简单的数字证书包含一个公开密钥、名称以及 CA 的数字签名。一般情况下，数字证书中还包括密钥的有效时间、发证机关(CA)的名称、该证书的序列号等信息，证书的格式遵循 ITUT X.509 国际标准。

数字证书采用公开密钥体制，即利用一对互相匹配的密钥进行加密、解密。每个用户自己设定一把特定的、仅为本人所知的专有密钥(私钥)，用它进行解密和签名；同时设定一把公共密钥(公钥)并由本人公开，用于加密和验证签名。使用数字证书可以保证以下安全。

- 信息除发送方和接收方外不被其他人窃取；
- 信息在传输过程中不被篡改；
- 发送方能够通过数字证书来确认接收方的身份；
- 发送方对于自己的信息不能抵赖；
- 信息自数字签名后到收到为止，未曾作过任何修改，签发的文件是真实文件。

2. 数字证书的作用

数字证书的作用主要表现在以下四个方面。

(1) 身份认证。身份认证即身份识别与鉴别，就是确认实体即为自己所声明的实体，其实现的主要方法是数字签名技术。如甲对乙的身份的认证是这样进行的：首先，甲要验证



乙的证书的真伪，当乙通过网络将证书传送给甲时，甲首先要用该证书的颁发机构 CA 的公钥解开证书上 CA 的数字签名，如签名通过验证，证明乙持有的证书是真的，而且从证书中得到的公钥确实是乙的；然后，甲要验证乙身份的真伪——即发件人是不是真实的乙？乙将文件用自己的私钥进行加密传送给甲，由于乙的公钥只能解开用乙的私钥加密的文件，因此，如果甲用乙的公钥可以解开该加密文件，即可证明发送该加密文件的人确实是乙本人。

(2) 数据完整性。数据完整性就是确认数据没有被修改，即数据无论是在传输或是在存储过程中经过检查确认没有被修改。数据完整性服务的实现主要方法也是数字签名技术。这是因为密码哈希算法和签名算法提供的保证，哈希算法的特点是输入数据的任何变化都会引起输出数据的不可预测的极大变化；签名是用自己的私钥将该哈希值进行加密，和数据一起传送给接收方。如果敏感数据在传输和处理过程中被篡改，接收方就不会收到完整的数据签名，验证就会失败。反之，如果签名通过了验证，就证明接收方收到的是没经修改的完整性数据。

(3) 数据保密性。数据保密性就是确保数据的秘密，除了指定的实体外，其他没经授权的人不能读出或看懂该数据。PKI 的保密性服务采用了“数字信封”机制，即发送方先产生一个对称密钥，并用该对称密钥加密敏感数据。同时，发送方还用接收方的公钥加密对称密钥，像装入一个“数字信封”里，然后将被加密的对称密钥(“数字信封”)和被加密的敏感数据一起传送给接收方。接收方用自己的私钥拆开“数字信封”，得到对称密钥，用对称密钥解开被加密的敏感数据。其他没经授权的人，因为没有拆开“数字信封”的私钥，看不见或读不懂原数据，起到了数据保密性的作用。

(4) 不可否认性。不可否认性服务是指从技术上实现保证实体对他们的行为的诚实性，即用数字签名的方法防止其对行为的否认。其中，人们更关注的是数据来源的不可否认性和接收的不可否认性，即用户不能否认敏感信息和文件不是来源于他；以及接收后的不可否认性，即用户不能否认他已接收到了敏感信息和文件。此外，还有其他类型的不可否认性，如传输的不可否认性、创建的不可否认性和同意的不可否认性等。

数字证书主要应用于各种需要身份认证的场合，它提供的安全服务能满足电子商务、电子政务、网上银行、网上证券等金融业交易的安全需求，是确保这些活动顺利进行必备的安全措施。

8.1.3 PKI 系统的基本组成

PKI 作为一组在分布式计算机系统中利用公钥技术和 X.509 证书所提供的安全服务，企业或组织可利用相关产品建立安全域，并在其中发布密钥和证书。在安全域内，PKI 管理加密密钥和证书的发布，并提供诸如密钥管理(包括密钥更新、密钥恢复和密钥委托等)、证书管理(包括证书产生和撤销等)和策略管理等。

PKI 在实际应用上是一套软硬件系统和安全策略的集合，它提供了一整套安全机制，使用户在不知道对方身份或分布地很广的情况下，以证书为基础，通过一系列的信任关系进行通信和电子商务交易。

一个典型的 PKI 系统如图 8-1 所示，其中包括 PKI 策略、软硬件系统、证书机构 CA、注册机构 RA、证书发布系统和 PKI 应用等。



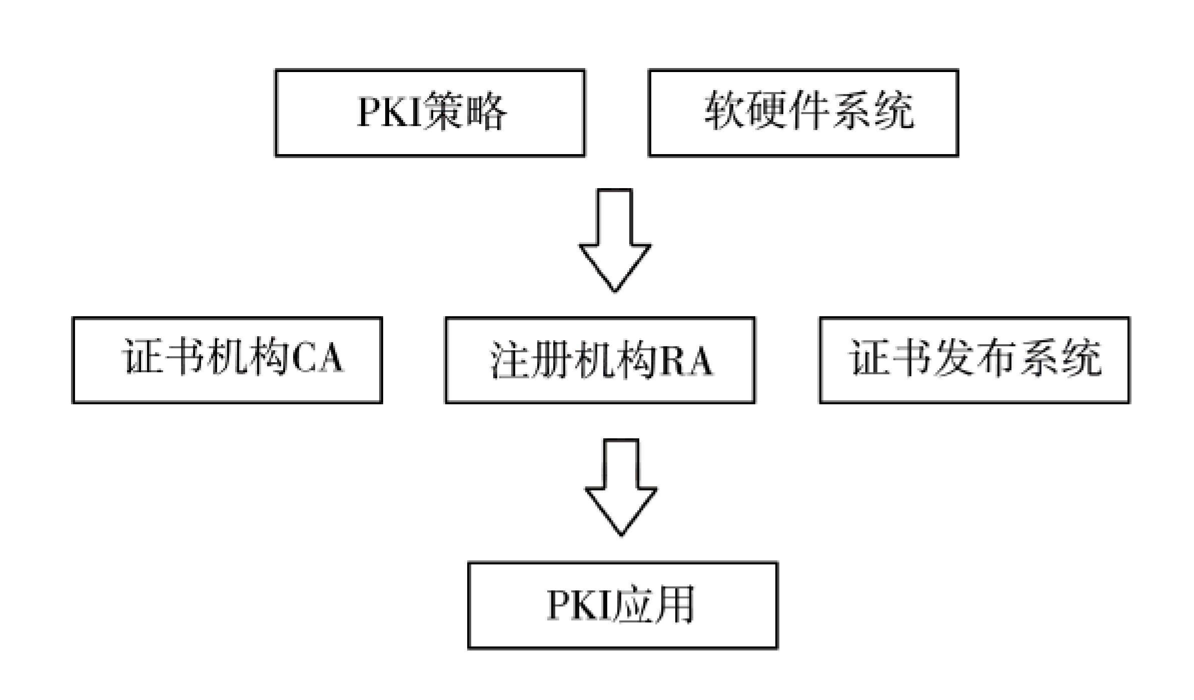


图 8-1　PKI 系统

- PKI 安全策略建立和定义了一个组织信息安全方面的指导方针，定义了密码系统使用的处理方法和原则。它包括一个组织怎样处理密钥和有价值的信息，根据风险的级别定义安全控制的级别。
- 证书颁发机构 CA 是 PKI 的信任基础，它管理公钥的整个生命周期，其作用包括：发放数字证书、规定数字证书的有效期和通过发布证书吊销列表（Certificate Revocation List，CRL）确保必要时可以废除证书。
- 注册机构 RA 提供用户和 CA 之间的一个接口，它获取并认证用户的身份，向 CA 提出证书请求。它主要完成收集用户信息和确认用户身份的功能。
- 证书发布系统负责证书的发放，如可以通过用户自己，或是通过目录服务。目录服务器可以是一个组织中现存的，也可以是 PKI 方案中提供的。
- PKI 的应用将在 8.1.5 小节做详细介绍。

8.1.4　Windows Server 2003 中的 PKI

利用 Windows Server 2003 家族的 PKI，可以帮助企业或组织实现以下主要功能。

1. 数字证书

数字证书是颁发机构所颁发的证明证书持有人身份的数字声明，它将公钥与拥有相应私钥的个人、计算机或服务绑在一起，提供身份验证、数据完整性和网络的安全通信。

2. 证书服务

在 Windows Server 2003 Standard Edition、Windows Server 2003 Enterprise Edition 和 Windows Server 2003 Datacenter Edition 上，证书服务是用于创建和管理证书颁发机构的组件。CA 负责建立和确定证书持有者的身份，如果证书不再有效，CA 会吊销证书。

3. 证书模板

数字证书是由 CA 根据证书申请中提供的信息和证书模板中包含的设置来颁发的。证书模板是针对接收到的证书申请应用的规则和设置的集合。对于企业的 CA 可以颁发的每一种类型的证书，都必须配置证书模板。



4. 证书自动注册

让计算机自动向企业证书颁发机构提交证书申请并安装颁发的证书,这有助于确保计算机能获得在组织内执行公钥加密操作所需的证书(例如,用于 Internet 协议安全性或客户端验证)。自动注册允许管理员配置受领人,以便自动注册证书,检索颁发的证书及延长过期的证书,而不需要受领人进行交互;不需要受领人具有证书操作方面的知识,除非证书模板被配置为与受领人进行交互。这大大地简化了客户使用证书的手续,并最大限度地减少了管理任务。

5. Web 注册页面

Web 注册页面是证书服务的单独组件,是安装 CA 时默认安装的,并允许证书申请者使用 Web 浏览器递交证书申请。

6. 智能卡支持

Windows 支持通过智能卡上的证书进行登录,以及使用智能卡来存储证书和私钥。智能卡可以用于进行 Web 身份验证、发送安全的电子邮件、无线网络和其他与公钥加密相关的活动中。

7. 公钥策略

在 Windows 中可以使用组策略自动给受领人颁发证书,建立可信的证书颁发机构及为 EFS 管理恢复策略。

8.1.5 PKI 的应用

PKI 技术的广泛应用能满足人们对网络交易安全保障的需求,并且在不断发展之中,下面给出几个应用实例。

1. 虚拟专用网络(Virtual Private Network,VPN)

VPN 是一种架构在公用通信基础设施上的专用数据通信网络,利用网络层安全协议(尤其是 IPSec)和建立在 PKI 上的加密与签名技术来获得机密性保护。基于 PKI 技术的 IPSec 协议现在已经成为架构 VPN 的基础,它可以为路由器之间、防火墙之间或者路由器和防火墙之间提供经过加密和认证的通信。

2. 安全电子邮件

作为 Internet 上最有效的应用,电子邮件凭借其易用、低成本和高效已经成为现代商业中的一种标准信息交换工具。随着 Internet 的持续增长,商业机构或政府机构都开始用电子邮件交换一些秘密的或是有商业价值的信息,这就引出了一些安全方面的问题,包括消息和附件可以在不为通信双方所知的情况下被读取、篡改或截掉;发信人的身份无法确认。电子邮件的安全也要求机密、完整、认证和不可否认,这些都可以利用 PKI 技术获得。

3. Web 安全

浏览 Web 页面是人们最常用的访问 Internet 的方式。如果要通过 Web 进行一些商业交易，该如何保证交易的安全呢？为了透明地解决 Web 的安全问题，在两个实体进行通信之前，先要建立 SSL(Secure Socket Layer，安全套接层协议)连接，以此实现对应用层透明的安全通信。利用 PKI 技术，SSL 协议允许在浏览器和服务器之间进行加密通信。此外，服务器端和浏览器端通信时双方可以通过数字证书确认对方的身份。结合 SSL 协议和数字证书，PKI 技术可以保证 Web 交易多方面的安全需求，使 Web 上的交易和面对面的交易一样安全。

4. 电子商务的应用

PKI 技术是解决电子商务安全问题的关键，综合 PKI 的各种应用，我们可以建立一个可信任和足够安全的网络。在通信中，利用数字证书可消除匿名带来的风险，利用加密技术可消除开放网络带来的风险，还可以使用一段可认证的完整数据表示的时间戳，这样，商业交易就可以安全可靠地在网上进行。

5. 应用编程接口 API

协议标准是系统具有可交互性的前提和基础，它规范了 PKI 系统各部分之间相互通信的格式和步骤。而应用编程界面 API(Application Programming Interfaces)则定义了如何使用这些协议，并为上层应用提供 PKI 服务。当应用需要使用 PKI 服务，如获取某一用户的公钥、请求证书废除信息或请求证书时将都会用到 API。目前 API 没有统一的国际标准，大部分都是操作系统或某一公司产品的扩展，并在其产品应用的框架内提供 PKI 服务。

8.2　密码技术

密码技术是信息交换安全的基础，通过数据加密、消息摘要、数字签名及密钥交换等技术实现了数据机密性、数据完整性、不可否认性和用户身份真实性等安全机制，从而保证了网络环境中信息传输和交换的安全。密码技术大致可以分为三类：对称密钥算法、非对称密钥算法(也称为公开钥密算法)和单向散列函数。

8.2.1　对称密钥算法

对称密钥算法是指加密和解密数据使用同一个密钥，即加密和解密的密钥是对称的。典型的对称密钥算法是 DES、IDEA 和 RC 等算法。对称密钥算法的特点是计算量小、加密效率高，但在分布式系统中应用时则存在着密钥交换和管理的问题。

对称密钥算法加密、解密流程如图 8-2 所示。



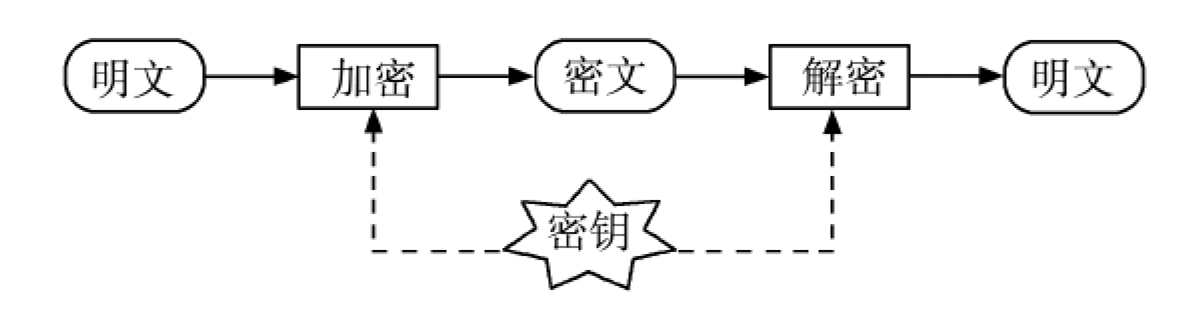


图 8-2　对称密钥算法加密、解密流程

1. DES 算法

DES(Data Encryption Standard,数据加密标准)是由 IBM 公司研制的,经长时间论证和筛选后,由美国国家标准局于 1977 年颁布的一种加密算法。DES 主要用于民用敏感信息的加密,1981 年被国际标准化组织接受作为国际标准。

DES 用于对 64 位的数据块进行加密和解密。它的密钥是 64 位,但其中包含 8 个比特的奇偶校验位,实际密钥长度是 56 位。DES 算法利用多次组合迭代算法和换位算法,对 64 位的数据块进行 16 轮编码。利用分散和错乱的相互作用,把明文编制成保密强度相对较高的密文。DES 算法的加密和解密的流程是完全相同的,区别仅是加密与解密使用子密钥序列的顺序正好相反。

DES 曾为全球贸易、金融等非官方部门提供了可靠的通信安全保障。它的缺点是密钥太短(56 位),影响了它的保密强度。此外,由于 DES 算法公开,其安全性完全依赖于对密钥的保护,必须有可靠的信道来分发密钥。因此,它不适合在网络环境下单独使用。

2. IDEA 算法

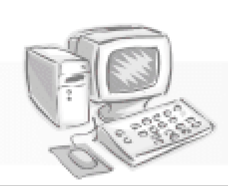
IDEA(International Data Encryption Algorithmic,国际数据加密算法)由著名密码专家来学嘉(瑞士籍华人)博士和 James L. Massey 于 1990 年联合提出。IDEA 算法是在 DES 算法的基础上发展起来的,也是一种数据块加密算法,明文和密文都是 64 位,但密钥长度为 128 位。IDEA 是作为迭代的分组密码实现的,使用 128 位的密钥和 8 个循环。

3. RC 系列算法

RC 系列算法是大名鼎鼎的 RSA 三人组设计的密钥长度可变的流加密算法,包括 RC2 算法、RC4 算法、RC5 算法和 RC6 算法。其中最流行的是 RC4 算法,RC 系列算法可以使用 2048 位的密钥,该算法的速度可以达到 DES 加密的 10 倍左右。

RC4 算法的原理包括初始化算法和伪随机子密码生成算法两大部分,在初始化的过程中,密钥的主要功能是将一个 256 字节的初始数簇进行随机搅乱,不同的数簇在经过伪随机子密码生成算法的处理后可以得到不同的子密钥序列,得到的子密钥序列和明文进行异或运算(XOR)后,得到密文。

由于 RC4 算法加密采用的是异或方式,所以,一旦子密钥序列出现了重复,密文就有可能被破解,但是目前还没有发现密钥长度达到 128 位的 RC4 算法有重复的可能性,所以,RC4 算法也是目前最安全的加密算法之一。



8.2.2　非对称密钥算法

对称密钥算法在加密、解密时使用同样的密钥,这些密钥由发送者和接收者分别保存。对称密钥算法的主要问题是密钥的生成、管理和分发都很复杂,特别是随着用户的增加,密钥的需求量成倍增加。如果网络中有 n 个用户,每两个用户之间都需要建立保密通信,则系统中所需的密钥总数达 $n(n-1)/2$ 个,当 n 较大时,这个数是很大的。同时为了安全的需要,通信双方要经常地更换密钥,如此大的密钥要经常地产生、分配与更换,其难度之大可想而知,有时甚至是不可能实现的。

1976 年,美国斯坦福大学的两名学者 W. Diffie 和 M. Hellman 根据单向函数的概念提出了公开密钥体制。它与对称密钥算法不同,公开密钥体制采用两个不同的密钥来对信息进行加密和解密,因此也称为"非对称密钥算法"。加密密钥是公开的,解密密钥是保密的,加密和解密算法都是公开的,但是要从加密密钥求解密密钥却非常困难。每个用户有一个对外的加密密钥(称为公钥)和对外保密的解密密钥(称为私钥)。典型的非对称密钥算法有 RSA、ECC 和 DSA 等。

非对称密钥算法加密、解密流程如图 8-3 所示。

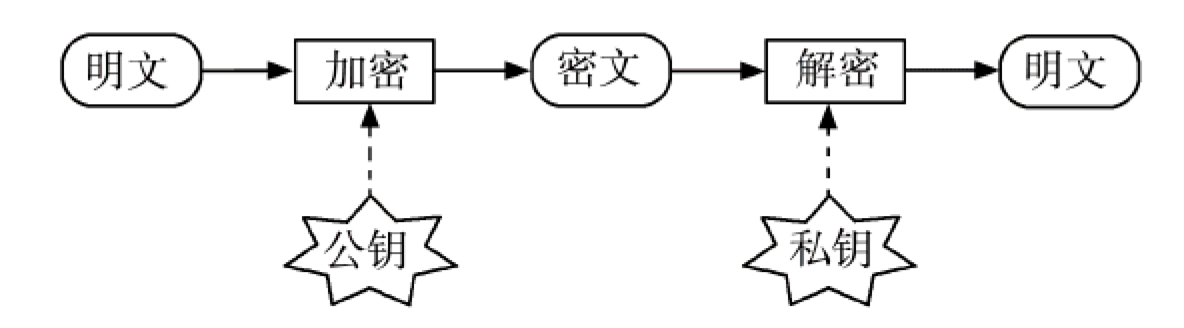


图 8-3　非对称密钥算法加密、解密流程

1. RSA 算法

RSA 公钥密码是 1977 年由 Ron Rivest、Adi Shamirh 和 Len Adleman 在美国麻省理工学院开发的,算法的名字以发明者的名字命名,是第一个既能用于数据加密也能用于数字签名的算法。RSA 是目前最有影响的公钥加密算法,它能够抵抗到目前为止已知的所有密码攻击,目前已被 ISO 推荐为公钥数据加密标准。

RSA 算法基于一个十分简单的数论事实:将两个大素数相乘十分容易,但是想分解它们的乘积却极端困难,因此可以将乘积公开作为加密密钥。

RSA 算法具有密钥管理简单(网上每个用户仅需保存一个密钥,且不需配送密钥)、可靠性高(取决于分解大素数的难易程度)等优点,但其算法复杂、加密解密速度慢,因此,通常被用于加密关键性的、核心的、少量的机密信息,而对于大量要加密的数据通常采用对称密钥算法。

2. ECC 算法

ECC(Elliptic Curves Cryptography,椭圆曲线密码编码学)由 Neal Koblity 和 Victor Miller 于 1985 年提出。ECC 算法的安全性基于椭圆曲线离散对数问题的计算困难性,将椭圆曲线中的加法运算与离散对数中的模乘运算相对应,将椭圆曲线中的乘法运算与离散



对数中的模幂运算相对应，即可以建立基于椭圆曲线的对应的密码体制。它的特点是抗攻击性强、计算量小、处理速度快。

3. DSA 算法

DSA(Digital Signature Algorithm，数字签名算法)是由美国 NIST(National Institute of Standards and Technoligy，美国国家标准技术研究院)作为 DSS(DigitalSignature Standard，数字签名标准)提出的。DSA 是一种基于公开密钥体制的数字签名算法，它不能用做加密，只用做数字签名。DSA 算法使用公开密钥，为接收者验证数据的完整性和数据发送者的身份，也可用于由第三方确定签名和所签数据的真实性。算法的安全性是基于解离散对数的困难性，这类签名标准具有较大的兼容性和适用性，成为网络安全体系的基本构件之一。

8.2.3 单向散列函数

在信息安全技术中，一般存在两个方向的加密方式：双向加密和单向加密。前面介绍的加密方式都属于双向加密，即将明文数据加密成不可理解的密文数据后，在需要的时候，可以使用一定的算法将这些密文恢复为原来的明文。而单向加密只对数据进行加密而不能进行解密，适用于不需要对信息解密或读取的情况，如验证用户输入的账号和密码是否正确。

单向散列(Hash)函数就是这类单向加密数据的函数，它对不同长度的输入消息，产生固定长度的输出。这个固定长度的输出称为原输入消息的“散列”或“消息摘要”(Message digest)，其长度取决于所采用的算法，通常在 128～256 位之间。

目前已提出的许多单向散列函数中，比较可靠而得到广泛使用的有 MD5 和 HA-1。

MD5(Message-Digest algorithm，消息-摘要算法)于 1991 年由 Rivest 开发出来，经 MD2，MD3 和 MD4 发展而来。MD5 克服了 MD4 的缺陷，生成 128 位的摘要信息串，出现之后迅速成为主流算法，并在 1992 年被收录到 RFC(Request For Comments，请求注解。可以把 RFC 理解为互联网协议的草案及标准，比如 HTTP 协议和 FTP 协议都是由 RFC 定义的)中。

SHA(Secure Hash algorithm，安全散列算法)于 1993 年由美国国家安全局 NSA (National Security Agency)设计，之后被美国 NIST 收录到美国的联邦信息处理标准 FIPS (Federal Information Processing Standard)中，成为美国国家标准。SHA(后来被称作 SHA-0)于 1995 被 SHA-1 替代，SHA-1 生成长度为 160 位的摘要信息串，虽然之后又出现了 SHA-224、SHA-256、SHA-384 和 SHA-512 等被统称为“SHA-2”的系列算法，但仍以 SHA-1 为主流。

安全的散列函数在设计时必须满足两个要求：其一是寻找两个输入得到相同的输出值在计算上是不可行的，这就是我们通常所说的抗碰撞性；其二是找一个输入，能得到给定的输出在计算上是不可行的，即不可从结果推导出它的初始状态。现在使用的重要计算机安全协议，如 SSL、PGP 都用散列函数来进行签名，一旦找到两个文件可以产生相同的压缩值，就可以伪造签名，给网络安全领域带来巨大隐患。

2004年8月17日的美国加州圣巴巴拉的国际密码学会议上，来自中国山东大学的王小云教授做了破译MD4、MD5、HAVAL-128和RIPEMD算法的报告，公布了MD系列算法的破解结果。宣告了固若金汤的世界通行密码标准MD5的堡垒轰然倒塌，引发了密码学界的轩然大波。在业界专家普林斯顿大学教授Edwards Felton的个人网站上，他说："MD5已经受了重伤，它的应用就要淘汰。SHA-1仍然活着，但也不会很长，必须立即更换SHA-1，但是选用什么样的算法，这需要密码研究人员达成共识。"

8.3　EFS　加　密

《信息周刊》2008年"中国信息安全调查"数据发现，安全威胁的增长令企业遭受到更猛烈的攻击，而且威胁手段更加多样，从威胁的趋势来看，针对数据库的攻击越来越多。在各类安全威胁中，企业最重视哪3类？病毒和蠕虫、间谍软件、垃圾邮件一直高居榜首。然而，《信息周刊》研究部调查显示，数据安全的危害性正在日益上升，如未经授权的雇员对文件或数据的访问、带有公司数据的可移动设备遗失或失窃等，但是这一点却并没有引起企业足够的重视。

信息技术市场调研公司高德纳公司(Gartner)不久前曾进行一项关于数据被窃的调查，结果显示只有25%的数据失窃是源于不法之徒的恶意攻击，60%是由于移动设备丢失或被窃，15%是源于其他原因。由于移动办公已经成为不可逆转的趋势，要商业人员减少使用U盘、笔记本电脑等移动IT设备是不现实的。CheckPoint软件技术有限公司安全顾问吴航表示，治本的方法是协助他们加强数据安全，即使用严谨的加密技术配合访问控制技术，令移动IT设备即使失窃，其存储的数据也会"守口如瓶"。

8.3.1　EFS概述

EFS(Encrypting File System，加密文件系统)是Windows 2000/XP/Server 2003系统中特有的一个实用功能，对于NTFS分区上的文件和文件夹可以直接加密保存。EFS的用户验证过程是在登录Windows时进行，只要登录到Windows，就可以打开任何一个被授权的加密文件，而不需要在使用前手动解密已加密的文件。

注意：使用EFS只能加密NTFS分区上的文件或文件夹，且不能加密压缩的文件或文件夹。

1. EFS原理及说明

(1) 如果一个用户对文件或文件夹进行了加密，那么只有这个用户可以访问这个文件或文件夹，其他没有访问权限的用户是不能访问这个被加密数据的。

(2) 对于已加密的数据进行移动或传输时，在移动或传输过程中数据是被解密的，待移动到相应的位置后再次被加密。如果加密数据被移动到了非NTFS分区，数据会被自动解密。

(3) EFS是基于公开密钥体制的，为了保障EFS的正常工作，它被内置了一个恢复方



案。在用户丢失了私钥时，故障恢复代理用户可以给已加密的数据解密，这样就极大地保障了加密数据的安全性。

2. EFS 证书

微软的 EFS 技术可以对计算机上的数据进行加密，并控制哪些人有权解密或恢复数据，有效地减小数据失窃的隐患。文件被加密后，即使攻击者能够物理访问计算机的数据存储器，也无法读取用户数据。所有用户都必须拥有 EFS 证书，才能运用 EFS 对数据进行加密和解密。此外，EFS 用户必须拥有在 NTFS 分区中修改文件的权限。EFS 包括两种类型的证书。

(1) 加密文件系统证书(可直接称为：EFS 证书)。该证书允许其持有者使用 EFS 加密和解密数据，普通的 EFS 用户使用此类证书。

(2) 文件恢复证书。该证书的持有者可以在整个域或其他范围内对任何人加密的文件和文件夹进行恢复。只有域管理员或极受信任的委托人(即数据恢复代理，也称故障恢复代理)可以持有该证书。

注意：要允许其他授权用户读取加密的数据，需要给他们私钥，或使其成为故障恢复代理。故障恢复代理可以在其范围内的域或组织单位中，解密所有的 EFS 加密文件，而无须加密文件或文件夹的用户的私钥。

8.3.2 用 EFS 对文件和文件夹加密

1. 用 EFS 对文件加密

用 EFS 对文件加密，具体操作步骤如下：

(1) 建立两个用户账户(如：Sanny 和 Ellen)，以 Sanny 账户登录系统(建议采用 Windows Server 2003 R2 EnterPrise Edition)。在资源管理器 NTFS 格式分区中找到要加密的文件并右击，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择【常规】选项卡，如图 8-4 所示。



图 8-4 【常规】选项卡

(2) 单击【高级】按钮，打开如图 8-5 所示的【高级属性】对话框。

(3) 选中【加密内容以便保护数据】复选框，单击【确定】按钮，将弹出如图 8-6 所示【加密警告】提示框。在此提示框中有两个单选按钮可供选择。

- 如果选中【加密文件及其父文件夹】单选按钮，则今后添加到该文件夹中的文件和子文件夹都将被自动加密。





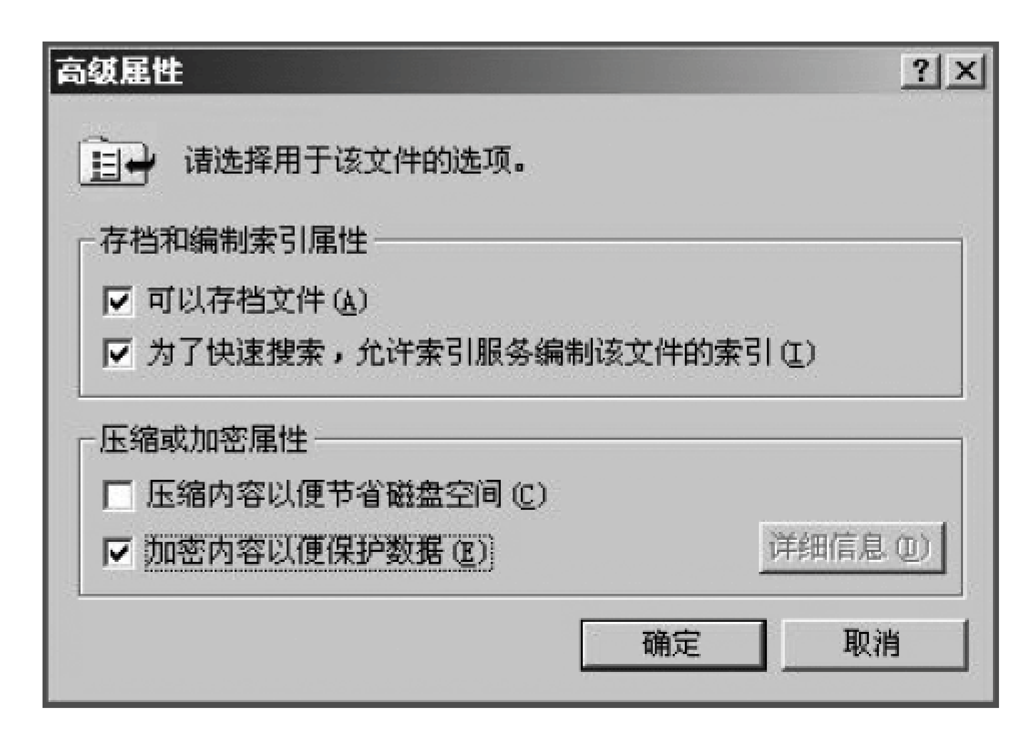


图 8-5　【高级属性】对话框

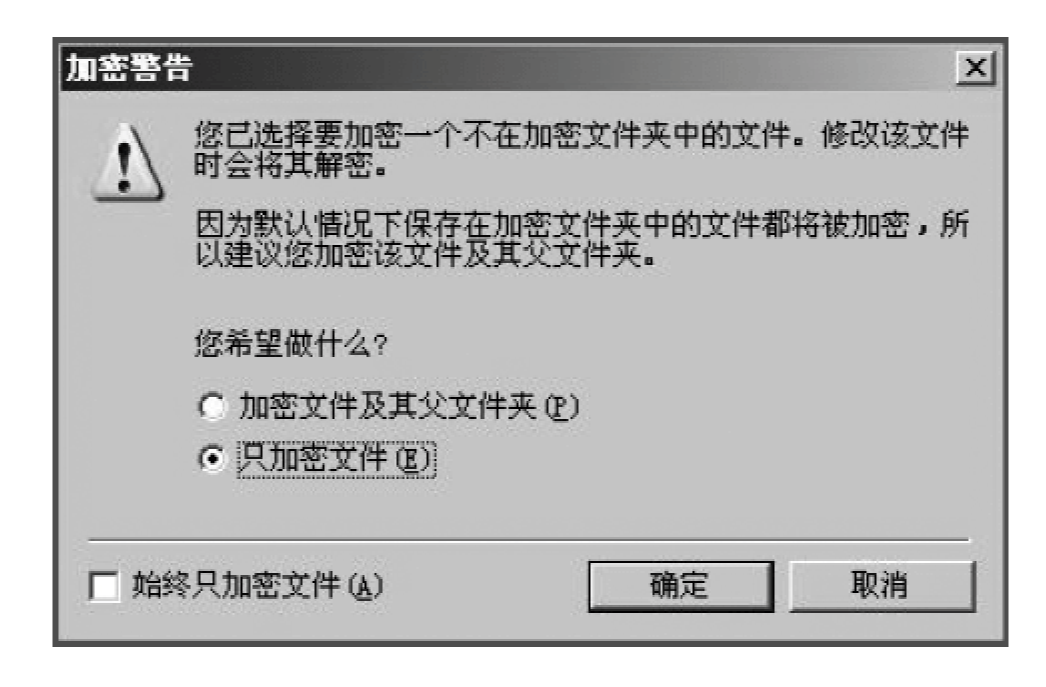


图 8-6　【加密警告】提示框

- 如果选中【只加密文件】单选按钮，则只会对选中的文件进行加密。

(4) 假设选中【只加密文件】单选按钮，单击【确定】按钮，完成文件的加密过程。加密后的文件名称以绿色字体显示，如图 8-7 所示。

(5) 双击加密文件，可以正常打开该文件。更换另一个用户(如：Ellen)重新登录，并试图打开该加密文件时，系统会弹出如图 8-8 所示【错误】提示框。



图 8-7　加密后的文件名称以绿色字体显示



图 8-8　【错误】提示框

注意：如果一个用户对文件或文件夹进行了加密，那么只有这个用户可以访问这个文件或文件夹，其他没有访问权限的用户是不能访问这个被加密数据的。

2. 文件夹加密

文件夹加密，具体操作步骤如下：

(1) 重新以 Sanny 账户登录系统，在资源管理器 NTFS 格式分区中找到要加密的文件夹并右击，然后在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择【常规】选项卡，如图 8-9 所示。

(2) 单击【高级】按钮，打开如图 8-10 所示的【高级属性】对话框。

(3) 勾选【加密内容以便保护数据】复选框，单击【确定】按钮，将弹出如图 8-11 所示【确认属性更改】提示框。在此提示框中有两个单选按钮可供选择(如果文件夹是空的，则不会出现提示)。



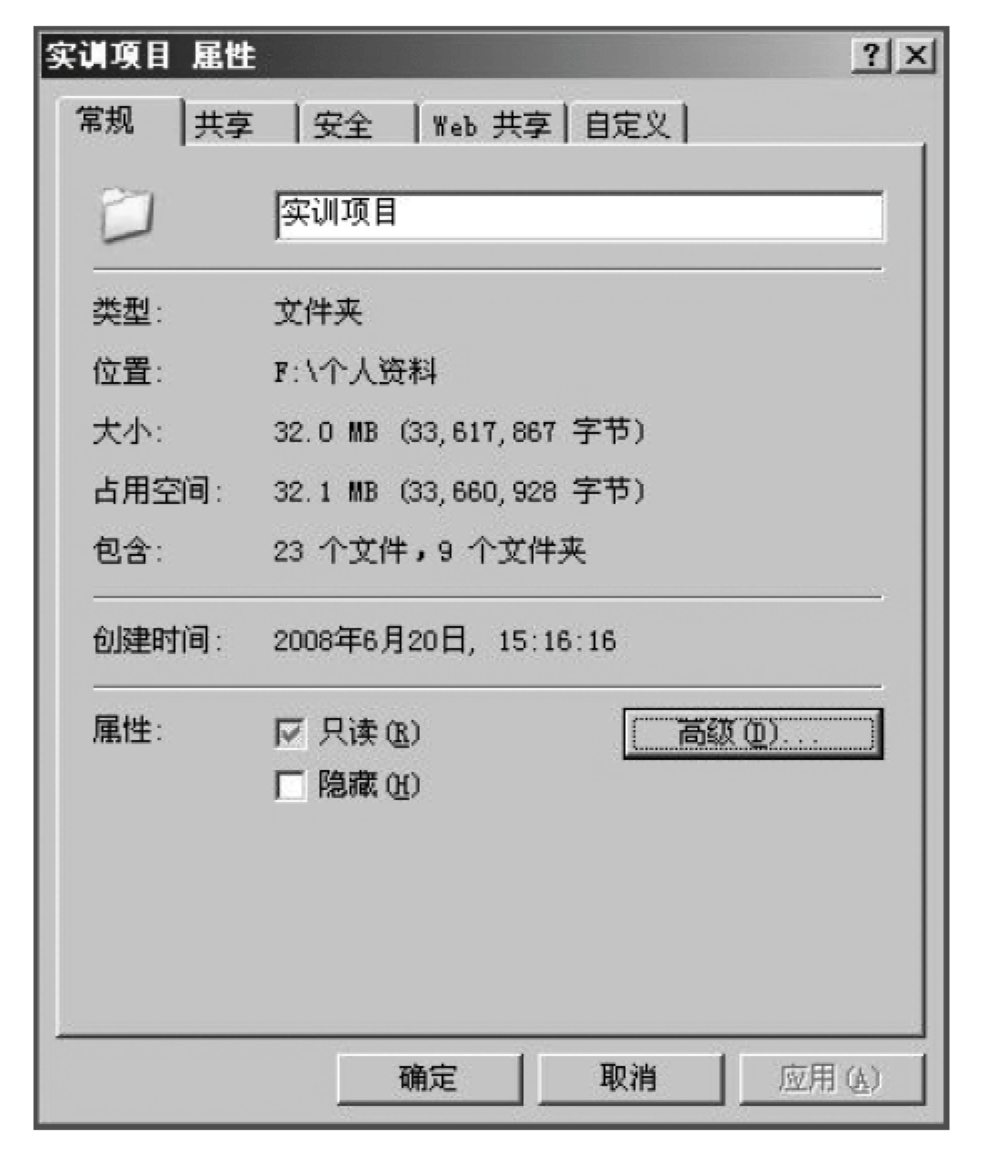


图 8-9 文件夹【属性】对话框的【常规】选项卡

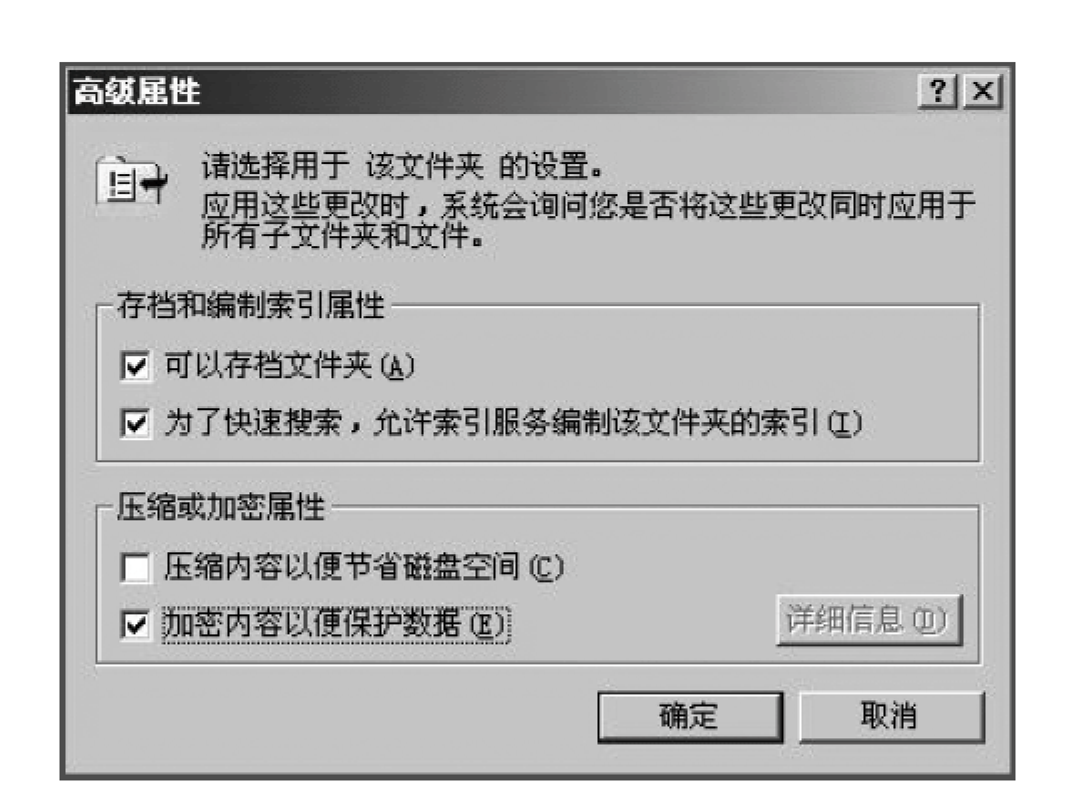


图 8-10 【高级属性】对话框

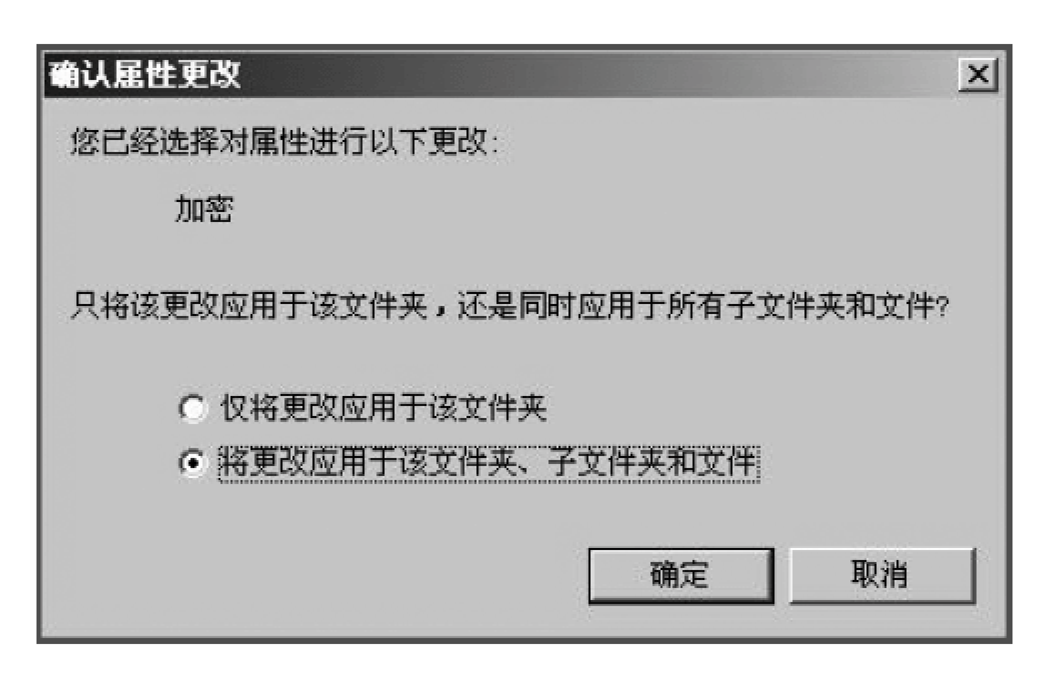


图 8-11 【确认属性更改】提示框

- 如果选中【仅将更改应用于该文件夹】单选按钮，那么该文件夹中现有的所有文件和子文件夹都不会被加密。但是，今后添加到该文件夹中的所有文件和子文件夹将被自动加密。
- 如果选中【将更改应用于该文件夹、子文件夹和文件】单选按钮，那么该文件夹中现有的所有文件和子文件夹以及今后添加到该文件夹中的文件和子文件夹都将被加密。

(4) 假设选中【将更改应用于该文件夹、子文件夹和文件】单选按钮，单击【确定】按钮，完成文件夹的加密过程。加密后的文件和文件夹名称以绿色字体显示(图 8-12)。

8.3.3 用 EFS 对文件和文件夹解密

用 EFS 对文件夹进行解密的操作步骤如下。

(1) 以 Sanny 账户登录系统，在已用 EFS 加密的文件夹上右击，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择【常规】选项卡，如图 8-9 所示。







图 8-12　加密后的文件和文件夹名称以绿色字体显示

(2) 单击【高级】按钮，打开如图 8-10 所示的【高级属性】对话框。取消选中【加密内容以便保护数据】复选框，然后单击【确定】按钮，返回到如图 8-9 所示的对话框。

(3) 单击【应用】或【确定】按钮，弹出如图 8-13 所示的【确认属性更改】提示框。在此提示框中有两个单选按钮可供选择。

- 如果选中【仅将更改应用于该文件夹】单选按钮，那么解密文件夹中的加密文件和文件夹仍保持加密。但是，在已解密文件夹内创立的新文件和文件夹将不会被自动加密。
- 如果选中【将更改应用于该文件夹、子文件夹和文件】单选按钮，那么将同时对该文件夹以及其下的子文件夹和文件进行解密。

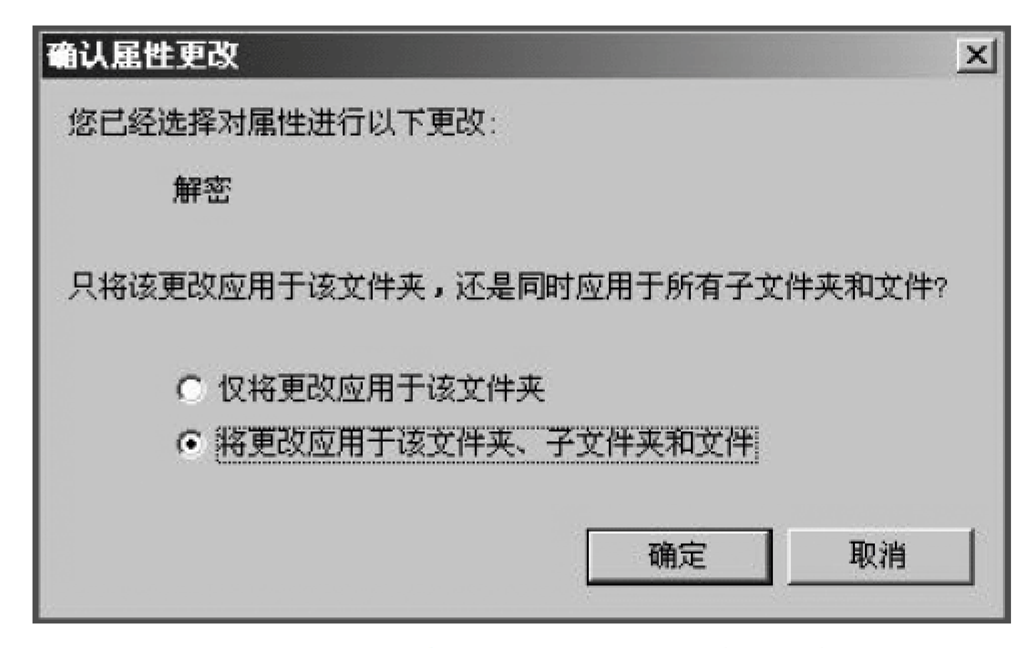


图 8-13　【确认属性更改】提示框

用 EFS 对文件进行解密的步骤与上述方法类似(略)。

8.3.4　启用 EFS 文件共享

企业通常希望使用加密技术以帮助保护敏感数据，但同时也允许多个用户访问这些数据。借助 EFS，用户就可以对文件进行加密，然后再授予其他用户访问这个加密数据的权限。要允许几个用户访问已加密的文件，这个文件的加密者就要把该文件设成共享状态，然后通过添加其他用户的 EFS 加密证书，允许他们共享访问这个加密的文件。这样，企业可以在提高安全性的同时，确保数据的可用性。

注意：此处共享的只是针对单个的加密文件，而不能是加密文件夹。所有添加到加密文件中的用户，必须在加密文件所在的计算机上拥有 EFS 加密证书。通常由 Verisign 等证书颁发机构颁发证书。此外，如果用户已经登录到计算机上并对其中的加密文件实施了解密，该用户将在这台计算机上拥有一份 EFS 加密证书。



具体操作步骤如下：

(1) 以 Administrator 账户登录系统，在资源管理器中要共享的加密文件（加密用户为 Administrator）上右击，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择【常规】选项卡，如图 8-14 所示。

(2) 单击【高级】按钮，打开如图 8-15 所示的【高级属性】对话框。

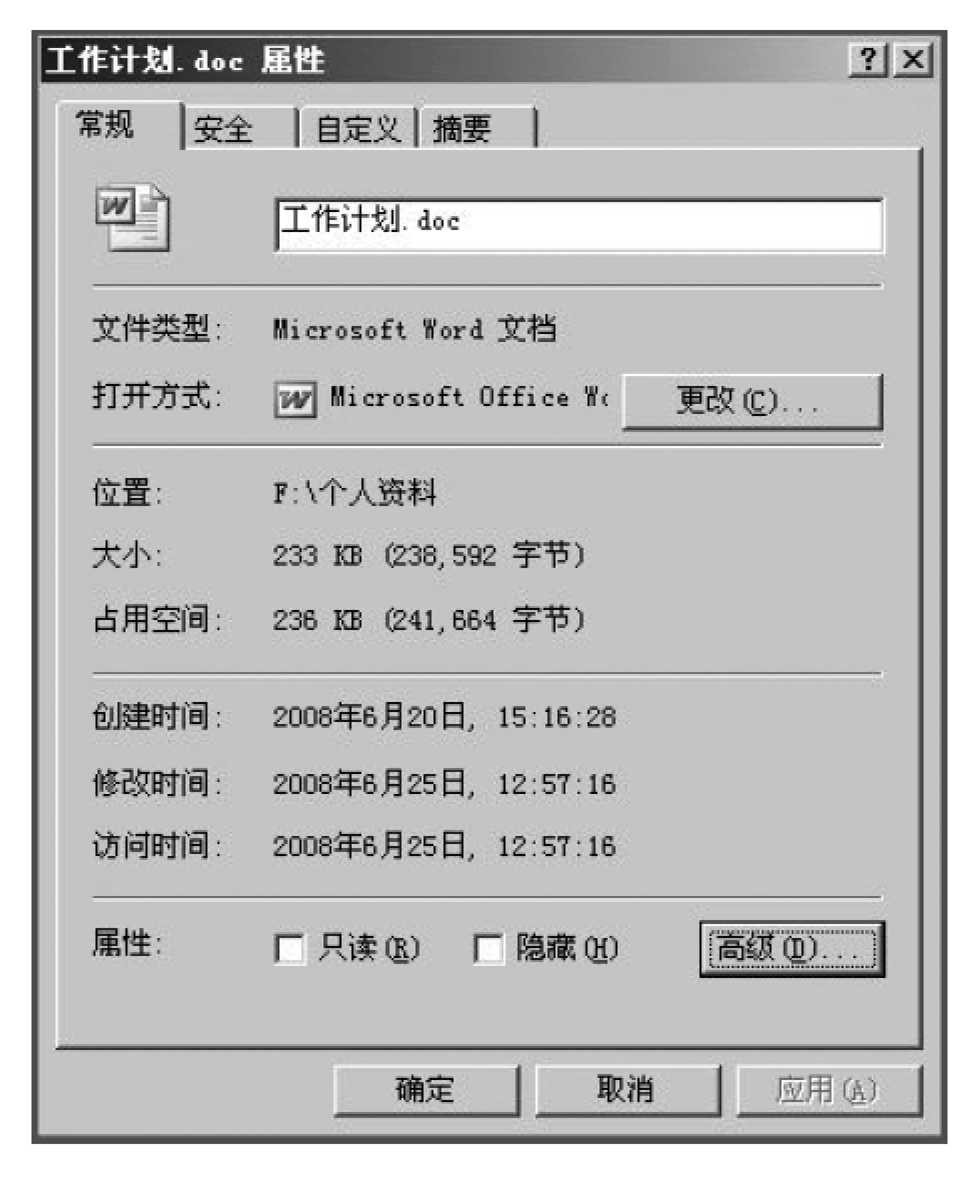


图 8-14　文件【属性】对话框的【常规】选项卡



图 8-15　【高级属性】对话框

(3) 单击【详细信息】按钮（如果是加密文件夹，则此按钮呈灰色状态不可选），打开如图 8-16 所示对话框。

(4) 如果要共享该文件的用户已在列表中，则直接选择相应用户，然后单击【确定】按钮即可。否则，单击【添加】按钮，打开如图 8-17 所示的【选择用户】对话框（一）。然后单击【寻找用户】按钮，在打开的对话框中单击【高级】按钮，接着单击【立即查找】按钮，打开如图 8-18 所示的【选择用户】对话框（二），选择相应用户账户（如 Ellen）。



图 8-16　【详细信息】对话框



图 8-17　【选择用户】对话框（一）





图 8-18　【选择用户】对话框(二)

(5) 单击【确定】按钮,选择的用户账户 Ellen 出现在如图 8-19 所示【选择用户】对话框(三)中,再单击【确定】按钮,即把相应账户添加到如图 8-17 所示对话框的列表中,如图 8-20 所示。



图 8-19　【选择用户】对话框(三)



图 8-20　添加新的共享用户后的【选择用户】对话框

如果此时想查看该用户的证书,单击【查看证书】按钮,打开【证书】对话框,在如图 8-21 所示的【常规】选项卡中可以查看该用户的基本 EFS 证书的创建和发布信息,在如图 8-22 所示的【详细信息】选项卡中可以更全面地了解该用户的基本 EFS 证书信息。

通过上述配置,所有在图 8-20 中列出的用户都可以共享该加密文件了。

注意:这里的"共享"是指可以在同一台计算机中允许多个用户访问由某一用户加密的文件,而不是指通过网络进行的"共享"。



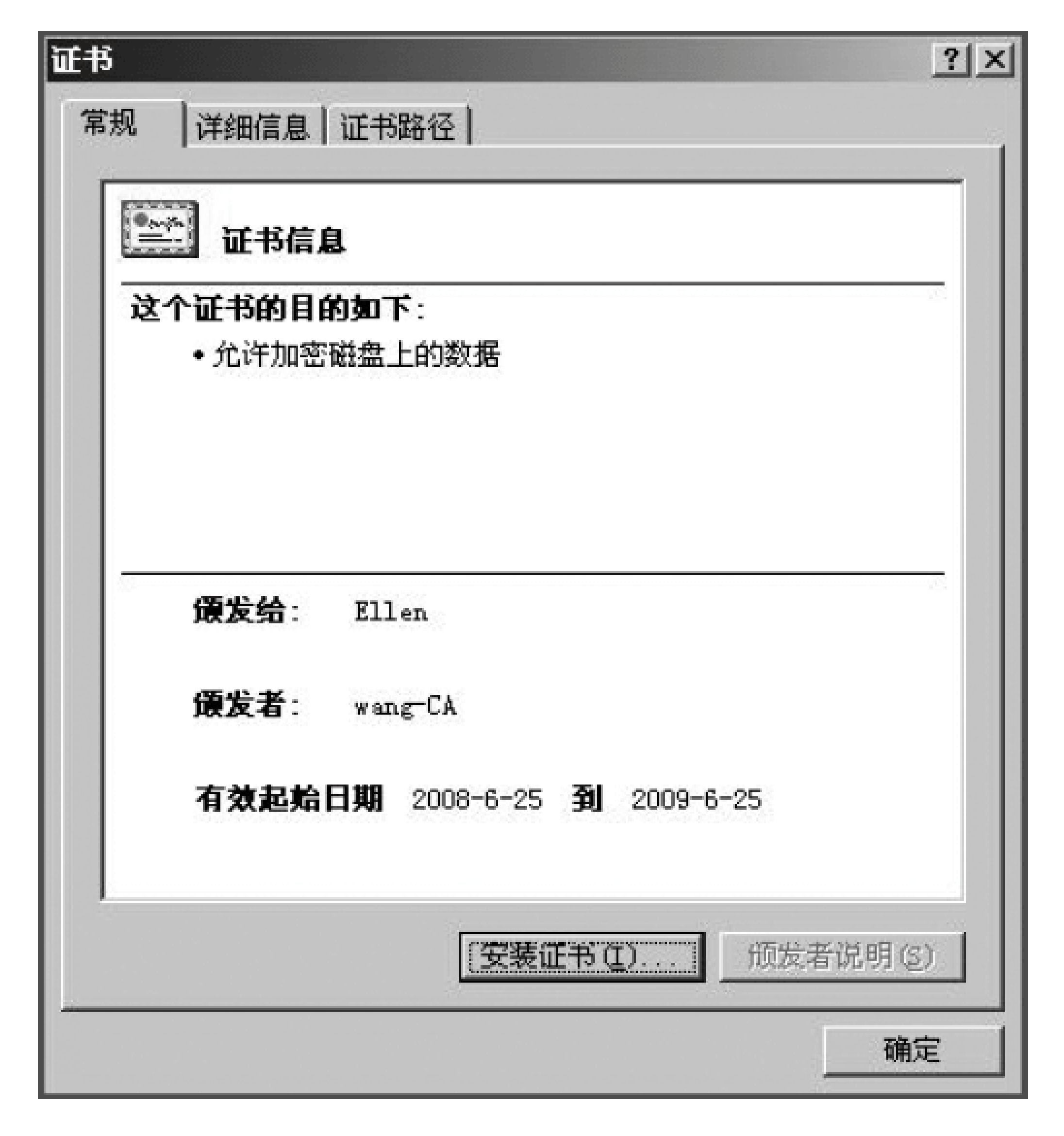





图 8-21 【证书】对话框的【常规】选项卡

图 8-22 【证书】对话框的【详细信息】选项卡

8.4 配置故障恢复代理

8.4.1 配置故障恢复代理概述

EFS 对文件或文件夹进行加密是依赖 PKI 中的公钥和私钥对(任何用户账户在创建后第一次登录系统时就会自动分配到一个公钥/私钥对)，公钥用来加密，私钥用来解密。作为 Windows 2000/XP/Server 2003 系统安全策略的一部分，通过故障恢复代理可以恢复加密的数据。例如，由于磁盘故障、自然灾害、用户遗忘或雇员离开公司等原因造成文件加密证书和相关私匙丢失，那么指定为故障恢复代理的人员可以进行数据的恢复。

1. 故障恢复代理

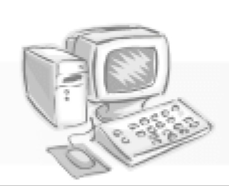
故障恢复代理是指获得授权解密由其他用户加密的数据的个人。在添加域故障恢复代理之前，必须确保每位故障恢复代理均获得了 X.509 v3 类型的证书。

如果用户是故障恢复代理，务必在 MMC(Microsoft Management Console，微软管理控制台)的【证书】中使用【导出】命令，将故障恢复证书和相关私钥备份到安全位置。备份完成后，应该使用 MMC 中的证书删除故障恢复证书。然后，在需要为用户执行故障恢复操作时，首先从 MMC 的【证书】中使用【导入】命令还原故障恢复证书和相关私钥。恢复数据之后，应该再次删除故障恢复证书，不必重复导出过程。要对域添加故障恢复代理，必须将他们的证书添加到现有的故障恢复策略中。

2. 故障恢复策略

恢复策略是单位的安全策略之一，目的在于出现意外时能够恢复加密文件。Windows





2000/Server 2003 分配有默认的恢复代理，Windows XP 系统没有。

故障恢复策略是为单独的计算机在本地组策略上配置的。对于网络中的计算机，可以在域、部门或单独计算机级别组策略上(图 8-23)配置故障恢复策略，并将其应用到策略可应用的所有基于 Windows XP/Server 2003 家族的计算机上。用户可以使用 MMC 中的【证书】来管理故障恢复证书。

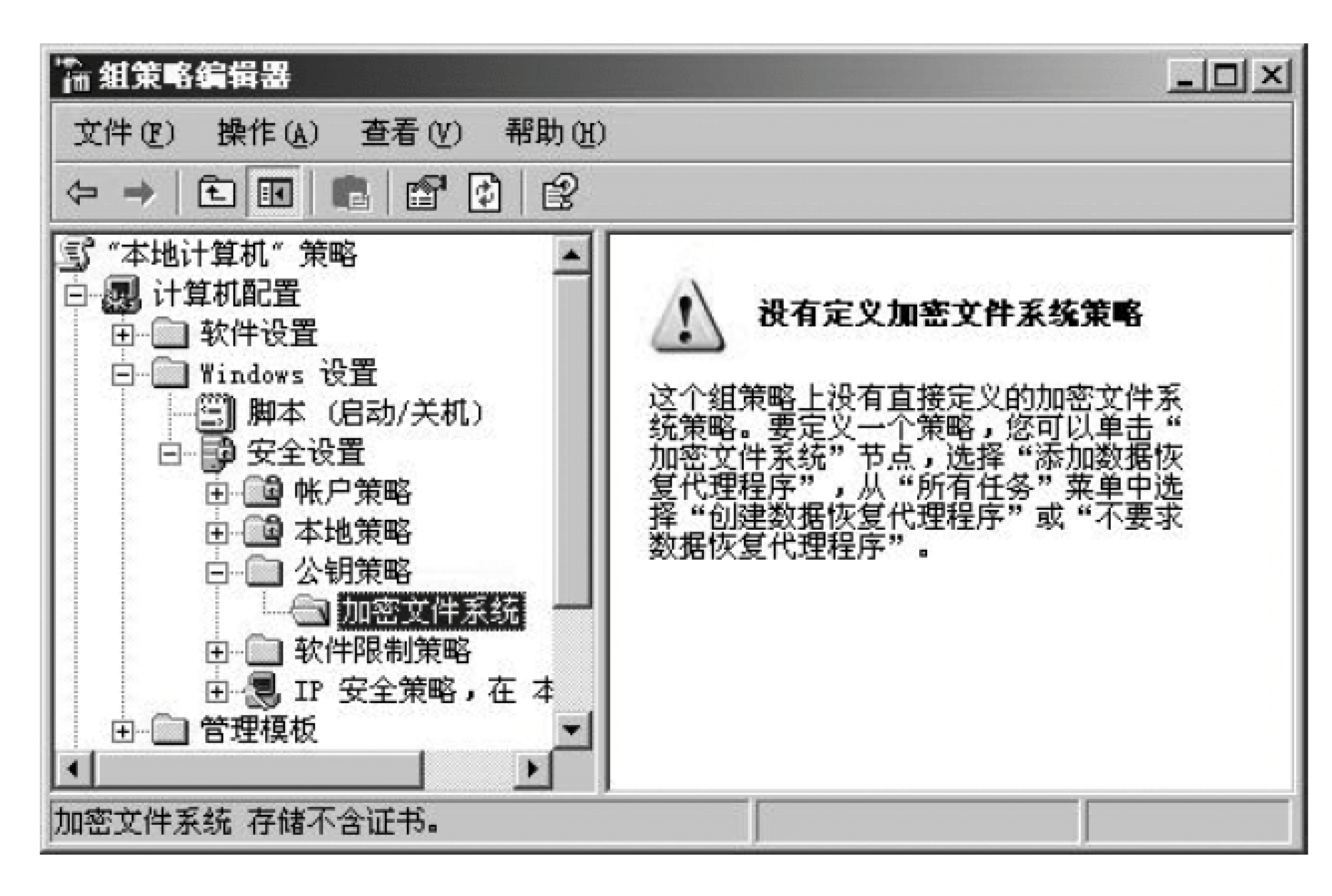


图 8-23　组策略中的故障恢复代理配置项

在域中，当设置第一个域控制器时，Windows Server 2003 家族执行该域的默认故障恢复策略。自行签署的证书将颁发给域管理员，将域管理员指定为故障恢复代理。要更改域的默认故障恢复策略，可以管理员身份登录到第一个域控制器，将其他故障恢复代理添加到本策略中，并且可以随时删除原始故障恢复代理。

8.4.2　配置故障恢复代理的步骤

配置故障恢复代理需要在域控制器中进行。具体步骤如图 8-24 所示。

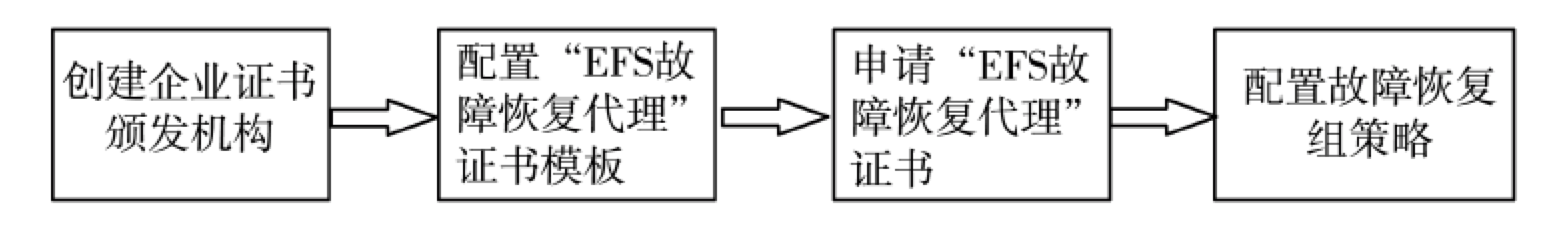


图 8-24　配置故障恢复代理的步骤

1. 创建企业证书颁发机构(CA)

在申请证书前必须在当前计算机中安装证书服务(该组件通过系统的"添加或删除程序"工具安装)，并配置企业 CA，然后申请证书。具体操作步骤如下：

(1) 以 Administrator 账户登录域控制器(建议采用 Windows Server 2003 R2 EnterPrise Edition)，在【控制面板】窗口中双击【添加或删除程序】图标，打开如图 8-25 所示的【添加或删除程序】窗口。

(2) 在左边的导航栏中单击【添加/删除 Windows 组件】按钮，打开如图 8-26 所示的【Windows 组件】对话框，选择【证书服务】选项。





图 8-25 【添加或删除程序】窗口



图 8-26 【Windows 组件】对话框

(3) 单击【下一步】按钮,系统会弹出如图 8-27 所示的【Microsoft 证书服务】提示框,提示安装了证书服务后,计算机名和域成员身份就不能改变了。

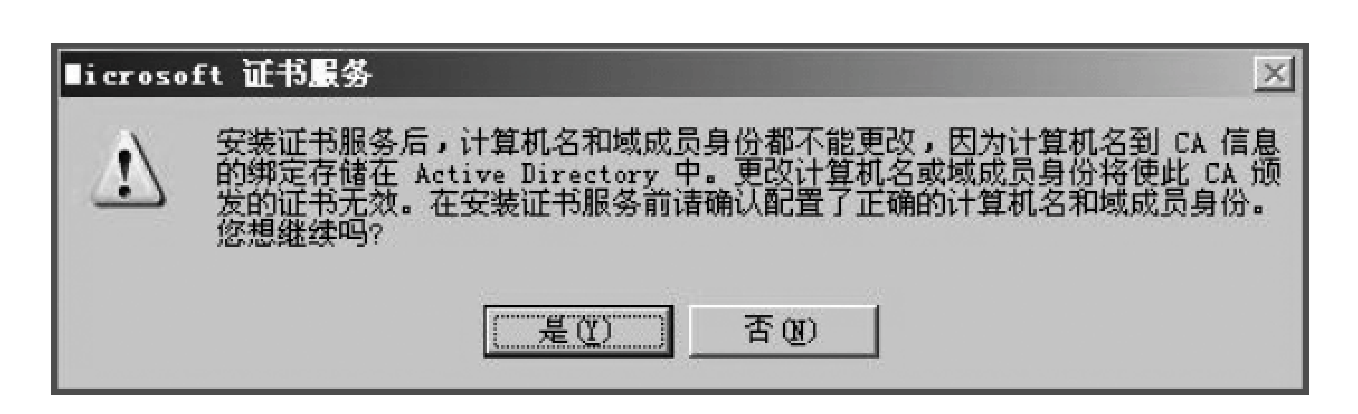


图 8-27 【Microsoft 证书服务】提示框

(4) 单击【是】按钮,打开如图 8-28 所示的【Windows 组件向导】对话框。这时要选择创建的企业 CA 的类型,由于安装证书服务需要创建企业根 CA,所以选择【企业根 CA】单选按钮。



(5) 单击【下一步】按钮，打开如图 8-29 所示的【CA 识别信息】对话框。在文本框中为创建的企业根 CA 取名，并对其进行简要说明，配置 CA 的有效期。



图 8-28　【Windows 组件向导】对话框



图 8-29　【CA 识别信息】对话框

(6) 单击【下一步】按钮，打开如图 8-30 所示的【证书数据库设置】对话框。在此要选择配置证书数据库和证书数据库日志文件所存放的路径，一般按默认设置即可。



图 8-30　【证书数据库设置】对话框

(7) 单击【下一步】按钮，系统会弹出如图 8-31 所示的【Windows 证书服务】提示框。提示用户在安装证书服务时，Internet 信息服务将暂停。



图 8-31　【Windows 证书服务】提示框



（8）单击【是】按钮，开始安装证书服务所需组件，并对证书服务数据库进行配置。完成后，在【管理工具】菜单下即可使用【证书颁发机构】命令了。此后用户即可申请自己的证书（包括本章所介绍的 EFS 故障恢复代理证书）。

2．配置“EFS 故障恢复代理”证书模板

通过配置【EFS 故障恢复代理】证书模板，添加指定的用户，使该用户具有使用该模板进行注册的权限。

具体操作步骤如下：

（1）在【运行】对话框中输入 certtmpl. msc 命令，打开【证书模板】控制台窗口，如图 8-32 所示。



图 8-32 【证书模板】控制台窗口

（2）在【EFS 故障恢复代理】证书模板上右击，在弹出的快捷菜单中选择【复制模板】命令，打开如图 8-33 所示的【新模板的属性】对话框。在【常规】选项卡的文本框中为新模板命名，并选中【在 Active Directory 中颁发证书】复选框。

（3）切换到【取代模板】选项卡，如图 8-34 所示。单击【添加】按钮，打开如图 8-35 所示的【添加取代模板】对话框。在其中选择原来的【EFS 故障恢复代理证书】模板，单击【确定】按钮，即把【EFS 故障恢复代理】证书模板添加到取代模板列表中，如图 8-36 所示。

（4）切换到【安全】选项卡，如图 8-37 所示。在默认情况下，可以注册密钥恢复代理证书模板的安全组只是 Domain Administrators 和 Enterprise Administrators 组。

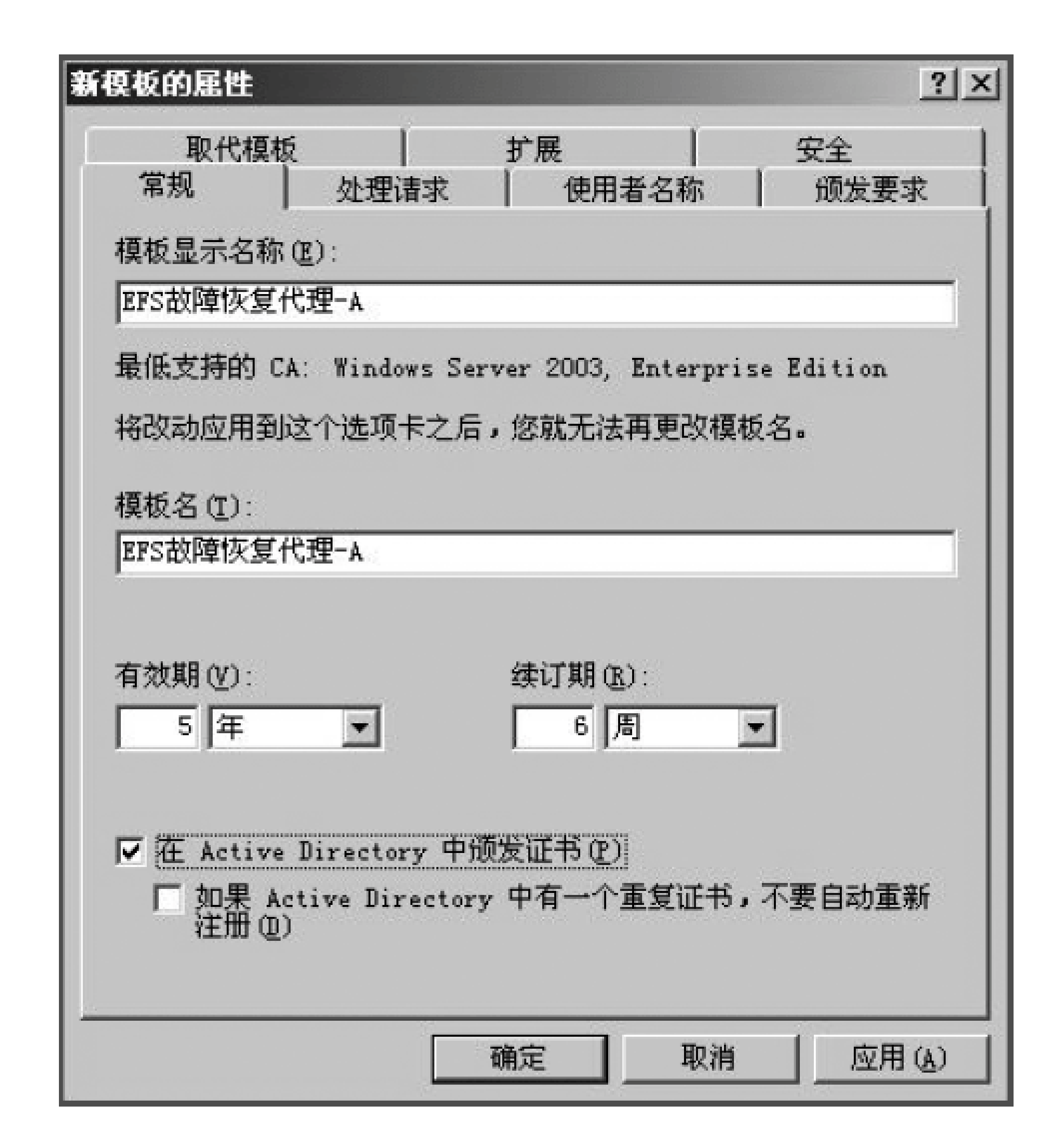


图 8-33 【新模板的属性】对话框的【常规】选项卡





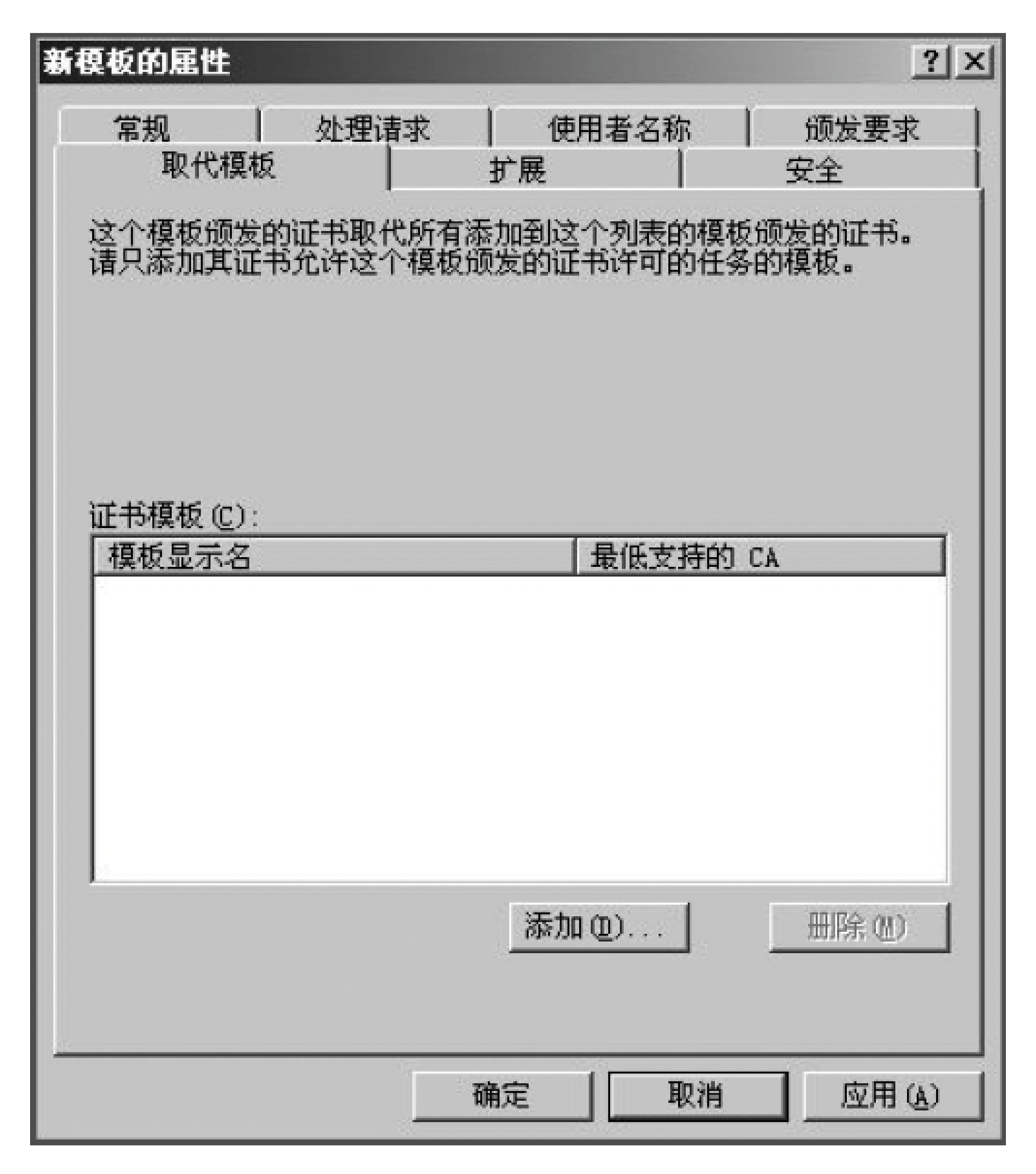


图 8-34　【取代模板】选项卡



图 8-35　【添加取代模板】对话框

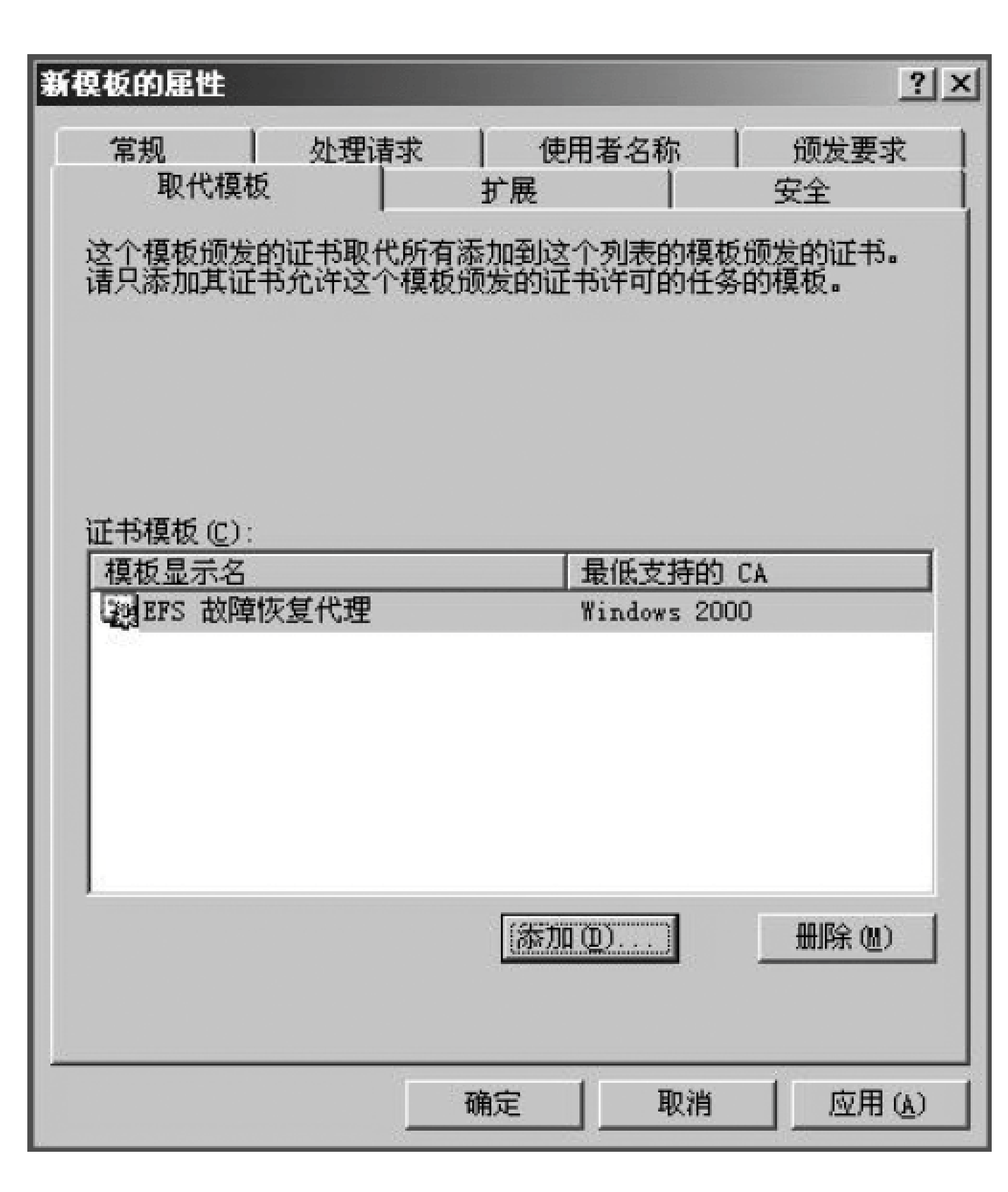


图 8-36　在【取代模板】选项卡中添加模板

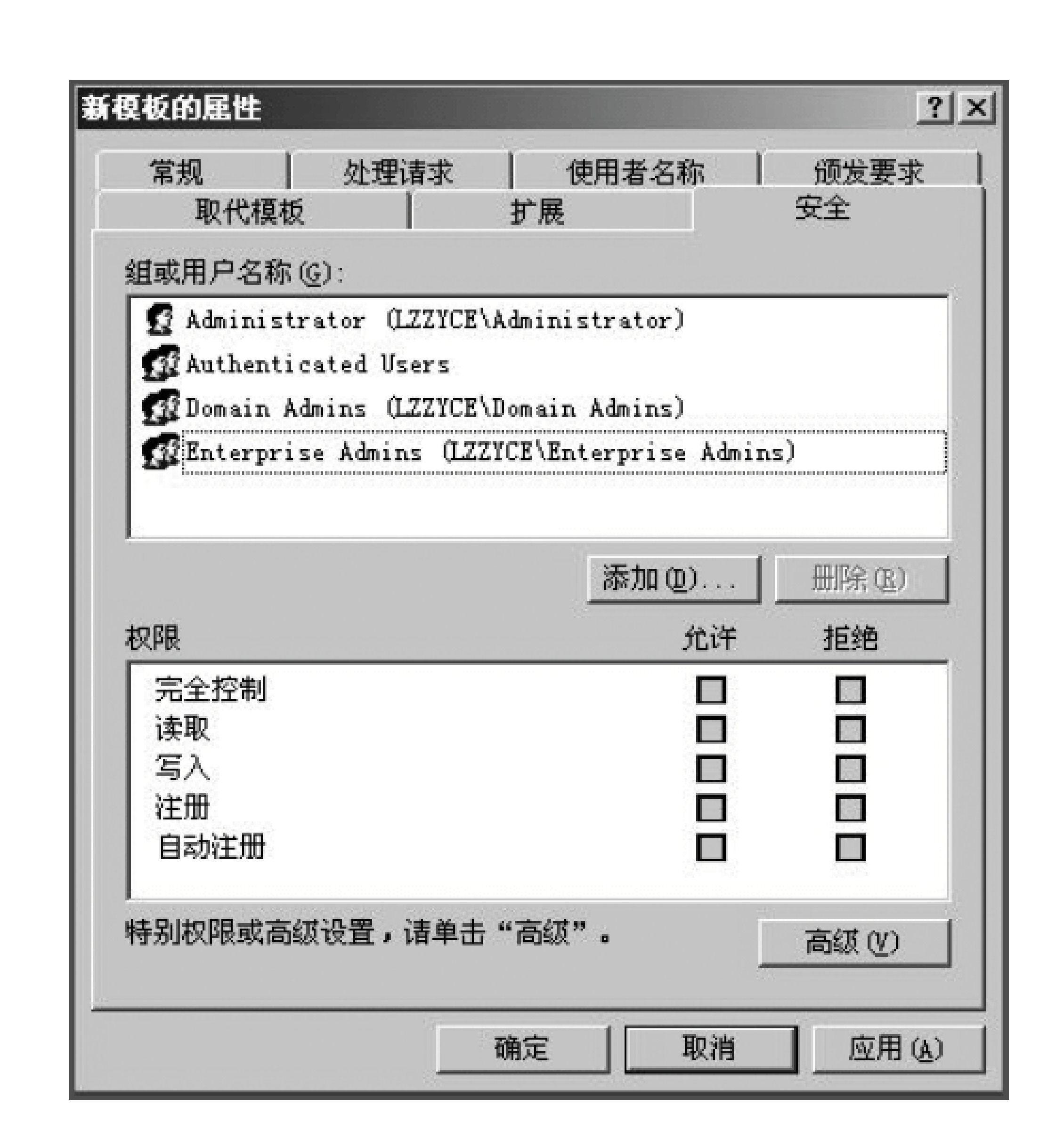


图 8-37　【安全】选项卡

（5）单击【添加】按钮，打开如图 8-38 所示【选择用户、计算机或组】对话框。在文本框中输入要成为故障恢复代理的用户账户（该账户必须在域中，如 Sanny）。单击【确定】按钮，返回到如图 8-37 所示的对话框中。此时已添加了新的账户，选择该账户，然后在下面的【Sanny 的权限】列表中选中【读取】和【注册】复选框，如图 8-39 所示。

（6）单击【确定】按钮，即完成模板的配置。下面可以由新添加的用户自己申请【EFS 故障恢复代理】证书模板了。



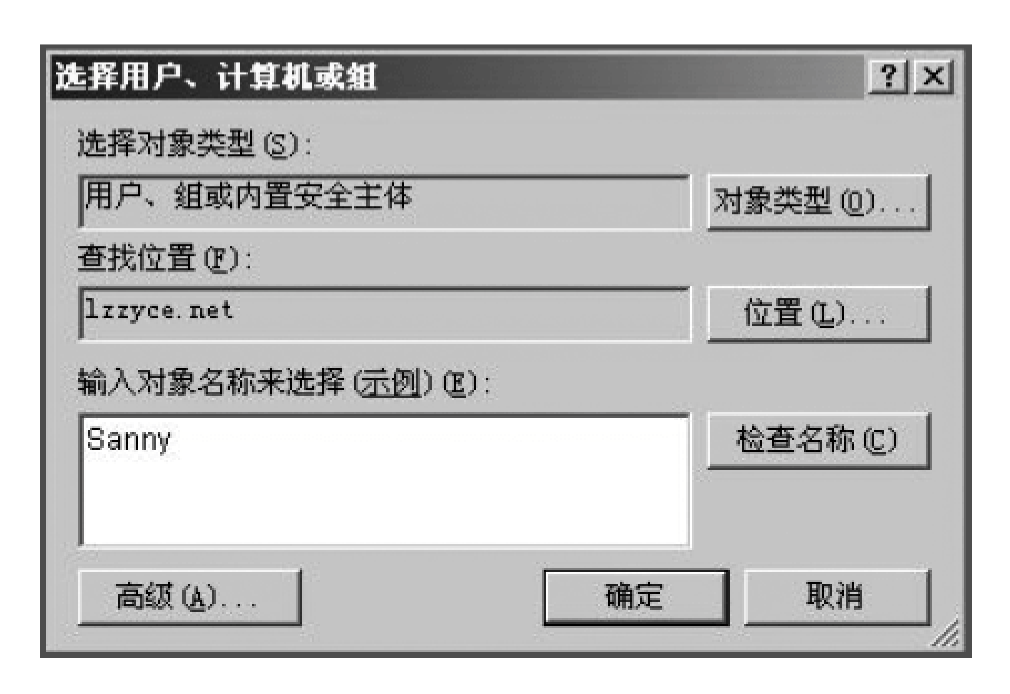


图 8-38 【选择用户、计算机或组】对话框

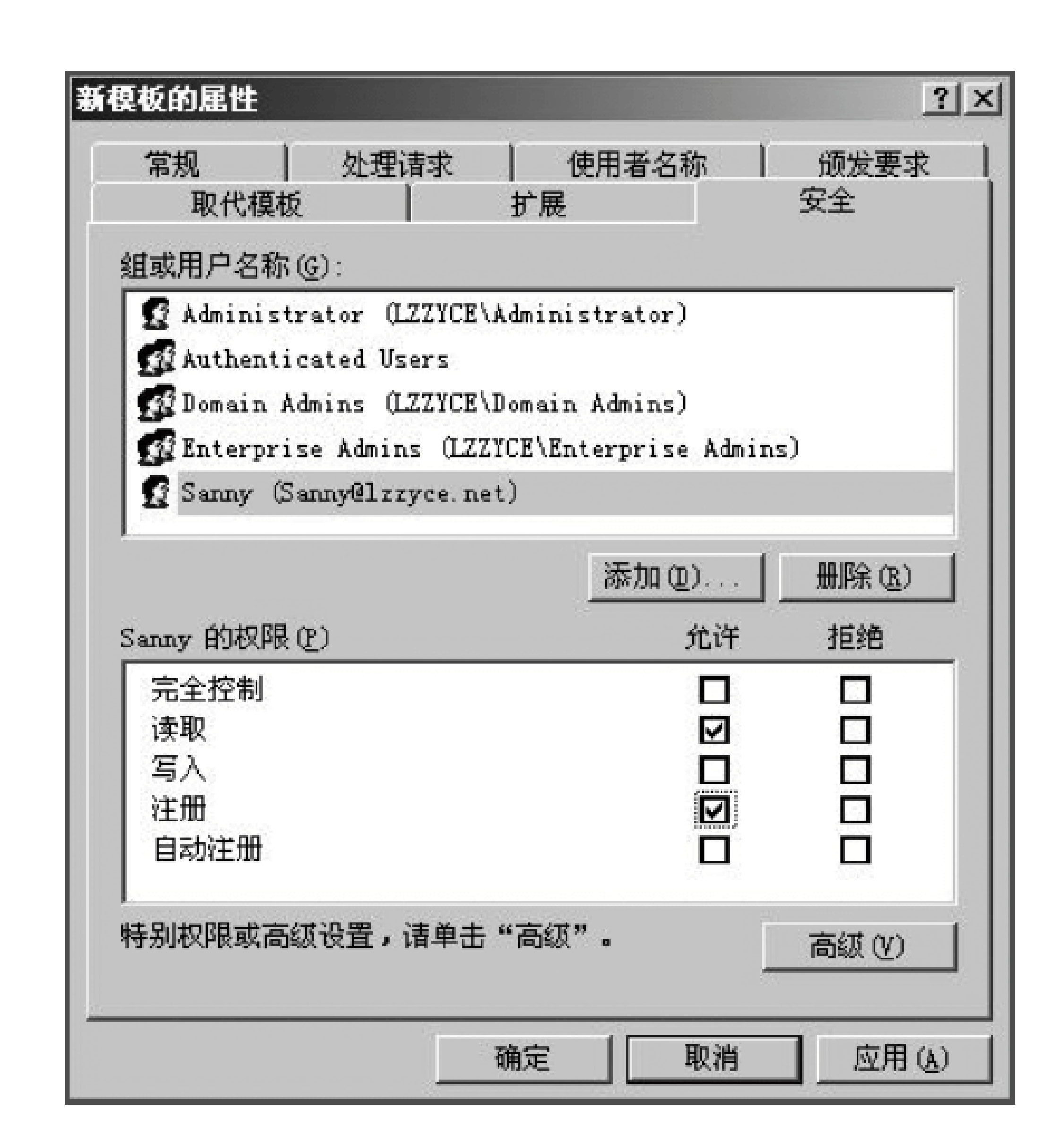


图 8-39 添加新用户后的【安全】选项卡

3. 申请 EFS 故障恢复代理证书

可以通过两种方法申请证书：证书申请向导方式和网页方式。

（1）方法一：以证书申请向导方式申请“EFS 故障恢复代理”证书模板。

这种方法分两步进行：首先添加证书管理单元，然后申请“EFS 故障恢复代理证书”模板。下面以 Sanny 账户登录域控制器为例说明。具体操作步骤如下：

① 在【运行】对话框中输入 MMC 命令，打开如图 8-40 所示【控制台】窗口。选择【文件】/【添加/删除独立管理单元】命令，打开如图 8-41 所示的【添加/删除管理单元】对话框。

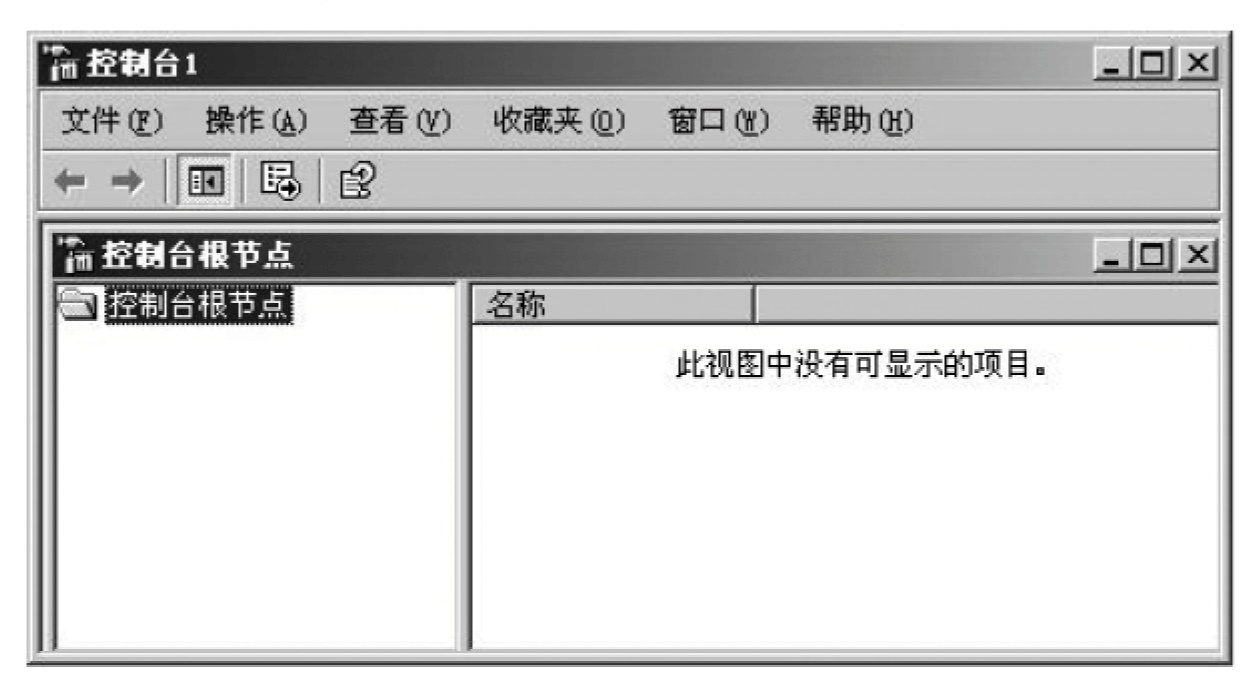


图 8-40 【控制台】窗口

② 单击【添加】按钮，打开如图 8-42 所示的【添加独立管理单元】对话框。在其中双击选择【证书】选项，打开如图 8-43 所示的【证书管理单元】对话框。在其中选择【我的用户账户】单选按钮。

③ 单击【完成】按钮，返回到如图 8-42 所示的对话框。然后单击【关闭】按钮，返回到如图 8-41 所示的对话框。最后单击【确定】按钮，返回到如图 8-40 所示的【控制台】窗口，此时已添加了【证书管理单元】，如图 8-44 所示。







图 8-41 【添加/删除管理单元】对话框



图 8-42 【添加独立管理单元】对话框



图 8-43 【证书管理单元】对话框



图 8-44 【证书】控制台

④ 接下来，申请“EFS 故障恢复代理证书”。在如图 8-44 所示控制台中选择【证书】/【个人】/【证书】选项，右击(图 8-45)并选择【申请新证书】命令，打开如图 8-46 所示的【欢迎使用证书申请向导】对话框。







图 8-45 【申请新证书】控制台

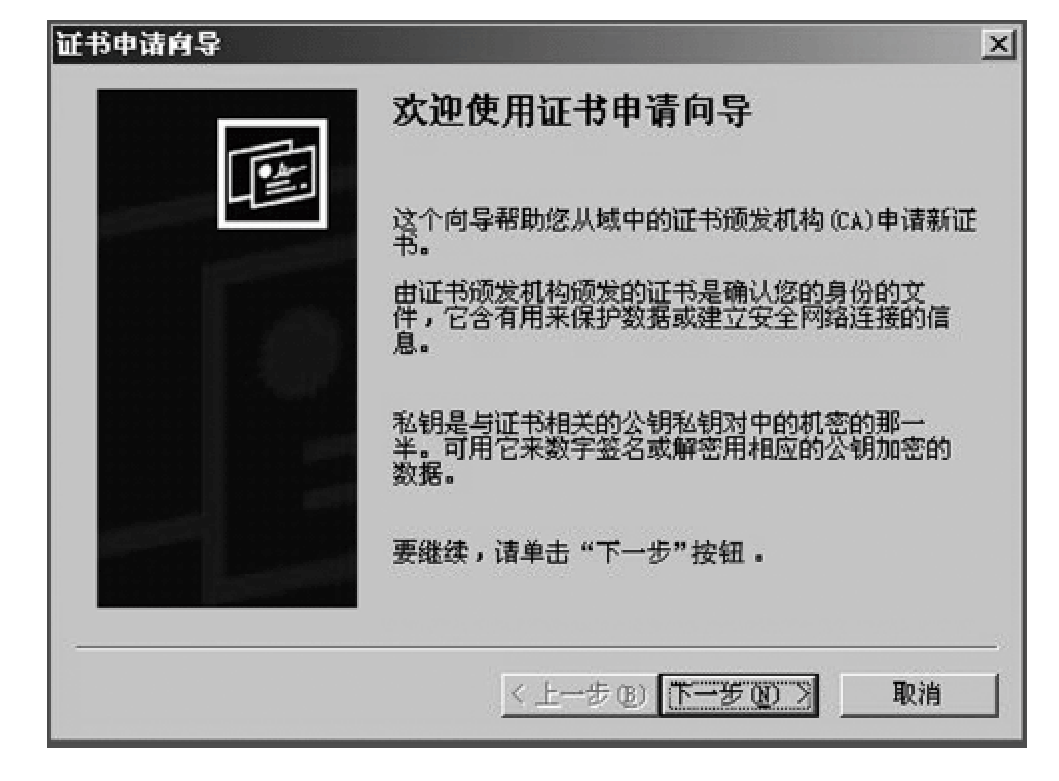


图 8-46 【欢迎使用证书申请向导】对话框

⑤ 单击【下一步】按钮，打开如图 8-47 所示【证书类型】对话框。在其中选择【EFS 故障恢复代理】选项（如果要对所申请的证书进行高级配置，则选中【高级】复选框）。

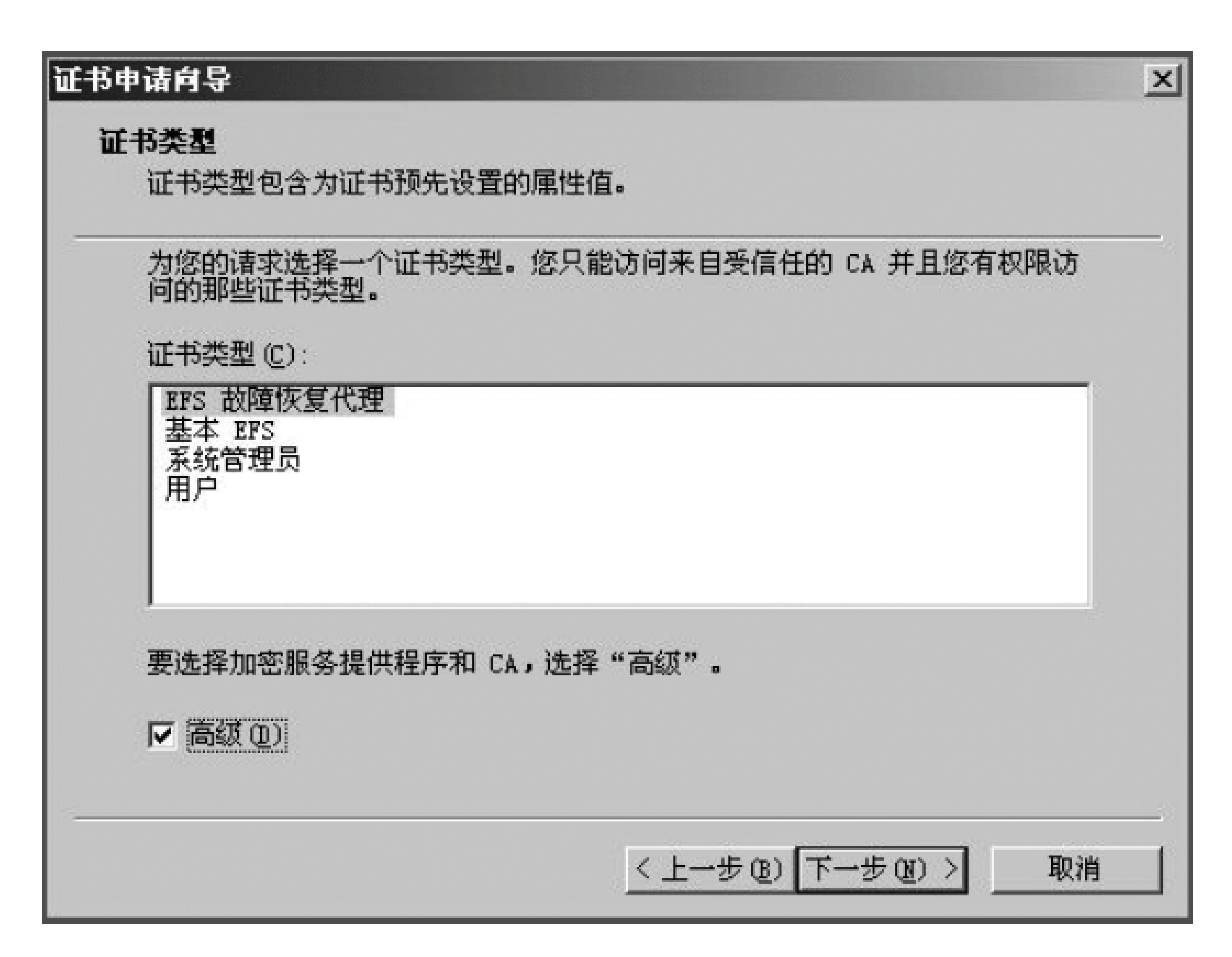


图 8-47 【证书类型】对话框

注意：如果没有进行前面的步骤（第 2 步：以 Administrator 账户登录系统，配置【EFS 故障恢复代理】证书模板，使 Sanny 账户具有使用该模板进行注册的权限），那么非系统管理员账户进行证书申请时，此步所出现的对话框如图 8-48 所示，其中没有【EFS 故障恢复代理】选项。

⑥ 在如图 8-47 所示的对话框中选中【高级】复选框，单击【下一步】按钮，打开如图 8-49 所示的【加密服务提供程序】对话框。选择 Microsoft Enhanced Cryptographic Provider v1.0（扩展加密服务提供程序）选项。还可选择与证书关联的公钥长度，如果希望启用强私钥保护，可选中【启用强私钥保护】复选框（启用强私钥保护将确保在每次使用私钥时都提示）。

⑦ 单击【下一步】按钮，打开如图 8-50 所示的【证书颁发机构】对话框。如果公司网络中具有多个可用的 CA，则通过单击【浏览】按钮选择所需 CA 的名称（如果只有一个 CA，则无须选择）。

⑧ 单击【下一步】按钮，打开如图 8-51 所示的【证书的好记的名称和描述】对话框。在文本框中为创建的“EFS 故障恢复代理证书”取一个好记的名字，并可进行适当的描述。



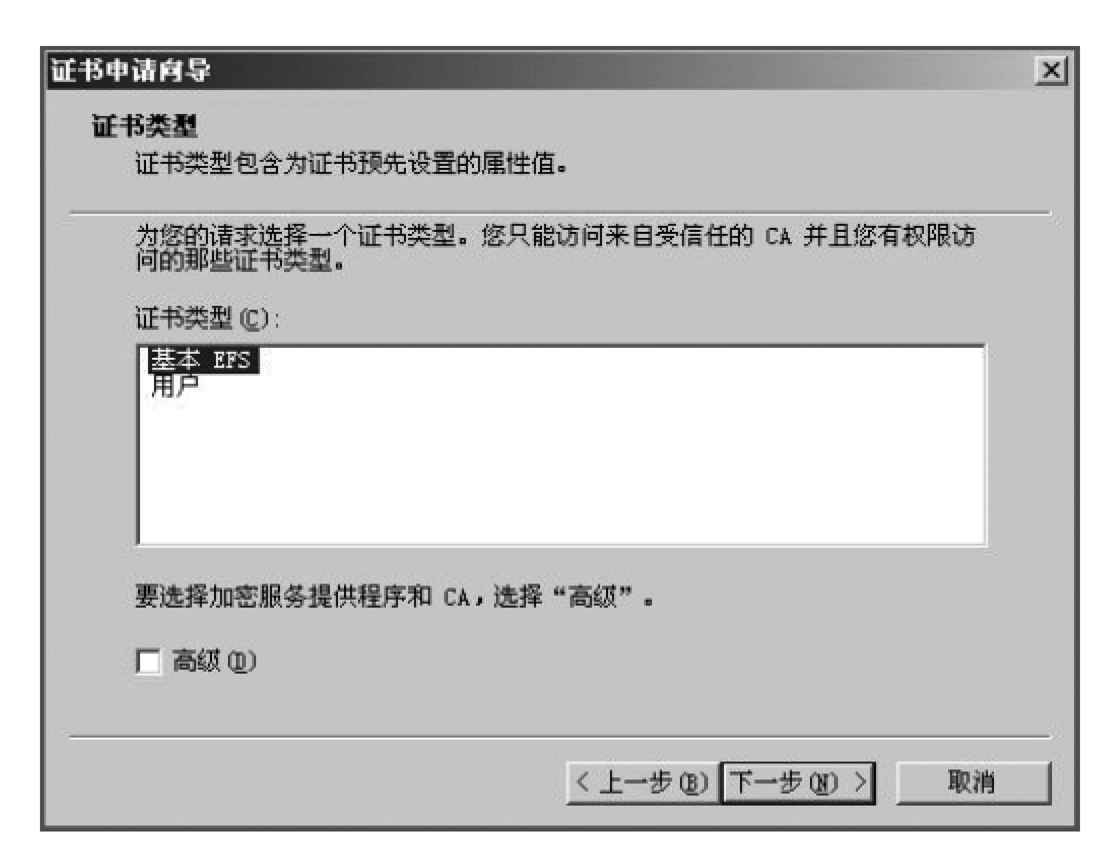


图 8-48　无注册权限用户的【证书类型】对话框

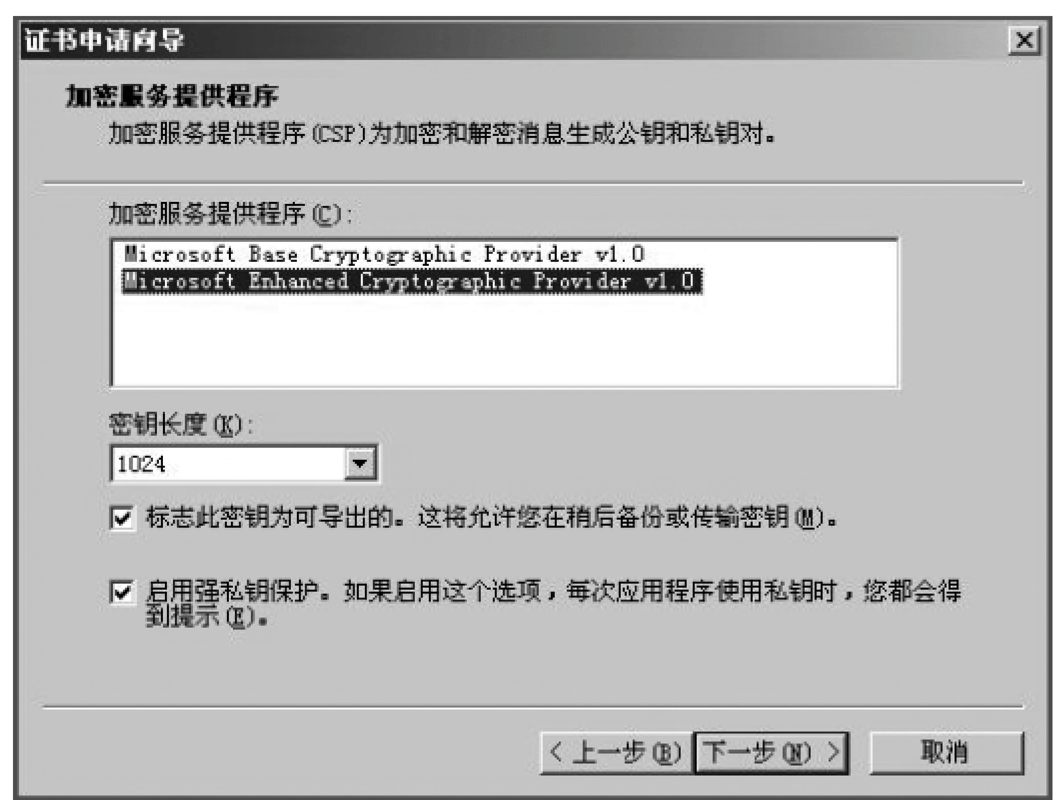


图 8-49　【加密服务提供程序】对话框



图 8-50　【证书颁发机构】对话框

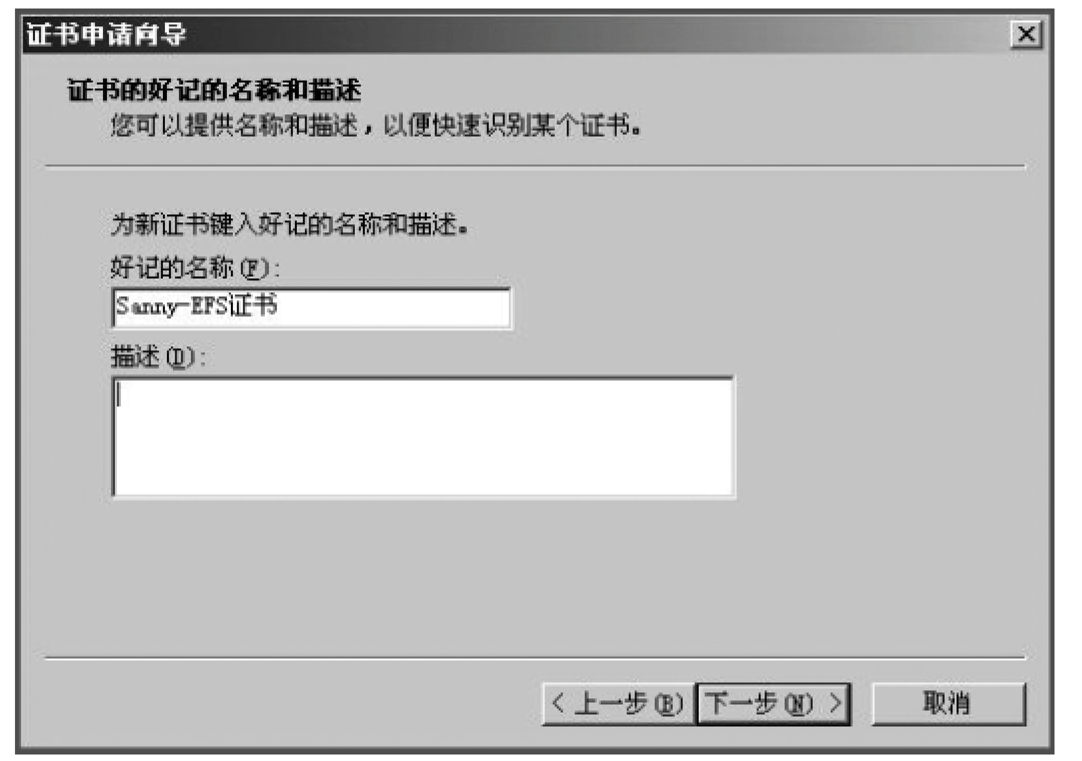


图 8-51　【证书的好记的名称和描述】对话框

⑨ 单击【下一步】按钮，打开如图 8-52 所示的【正在完成证书申请向导】对话框。其中显示了向导配置的摘要(如果觉得某项配置不正确，可以通过单击【上一步】按钮返回到相应步骤重新配置)。



图 8-52　【正在完成证书申请向导】对话框



⑩ 单击【完成】按钮，打开如图 8-53 所示的【应用程序正在创建受保护的项目】对话框，提示正在创建受保护的私钥。如果要设置私钥的安全级别，则单击【设置安全级别】按钮，在打开如图 8-54 所示的【选择适合于这个项目的安全级别】对话框中进行设置。再单击【下一步】按钮，回到如图 8-53 所示的对话框。单击【确定】按钮，系统会弹出【证书申请成功】提示框。



图 8-53 【应用程序正在创建受保护的项目】对话框



图 8-54 【选择适合于这个项目的安全级别】对话框

创建后的“EFS 故障恢复代理证书”会在【证书服务】控制台的【证书-当前用户】/【个人】/【证书】列表中显示，如图 8-55 所示。

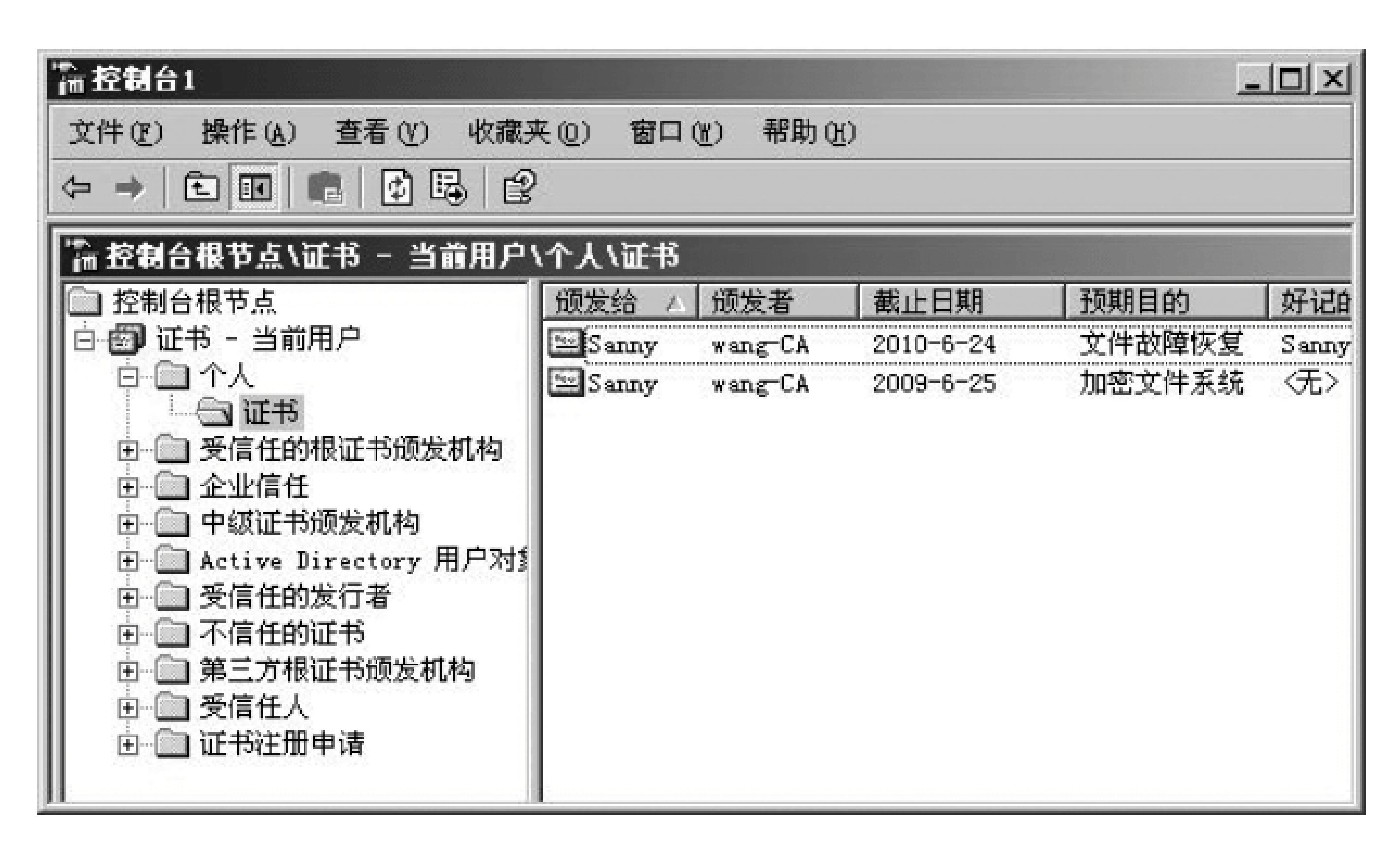


图 8-55 申请的“EFS 故障恢复代理证书”

(2) 方法二：以网页方式申请“EFS 故障恢复代理”证书。

默认情况下，每一个 Windows Server 2003 证书颁发机构 CA 都有可供用户和管理员使用的网页。这些页面可用于执行与申请证书相关的多种任务，该网页位于 http://servername/certsrv，其中 servername 是主持 CA 的服务器名称(或该服务器的 IP 地址)。

注意： http://servername/certsrv 中的 certsrv 部分应该用小写字母，否则，在检查和获取证书时可能出问题。用户可使用 IE 5.0 和更高版本，或 Netscape Navigator 3.01和更高版本来访问这些网页。

对于向独立 CA 申请证书的用户，网页方式是唯一的申请途径。对于向企业 CA 申请证书的用户，网页方式是可选的，还可以通过前面介绍的证书申请向导方式进行。



具体操作步骤如下：

① 以 Sanny 账户登录域控制器，打开浏览器，在地址栏中按 http://servername/certsrv 格式输入（如：http://192.168.1.53/certsrv），打开如图 8-56 所示的【身份验证】对话框。在其中输入故障恢复代理的用户名和密码。



图 8-56　【身份验证】对话框

② 单击【确定】按钮，进入证书申请网页首页，如图 8-57 所示。

③ 单击【申请一个证书】链接，打开如图 8-58 所示的【申请一个证书】页面。

④ 单击【高级证书申请】链接，打开如图 8-59 所示的【高级证书申请】页面（一）。通过【高级选项】的选择，允许在证书申请上赋予用户更大的控制权限。

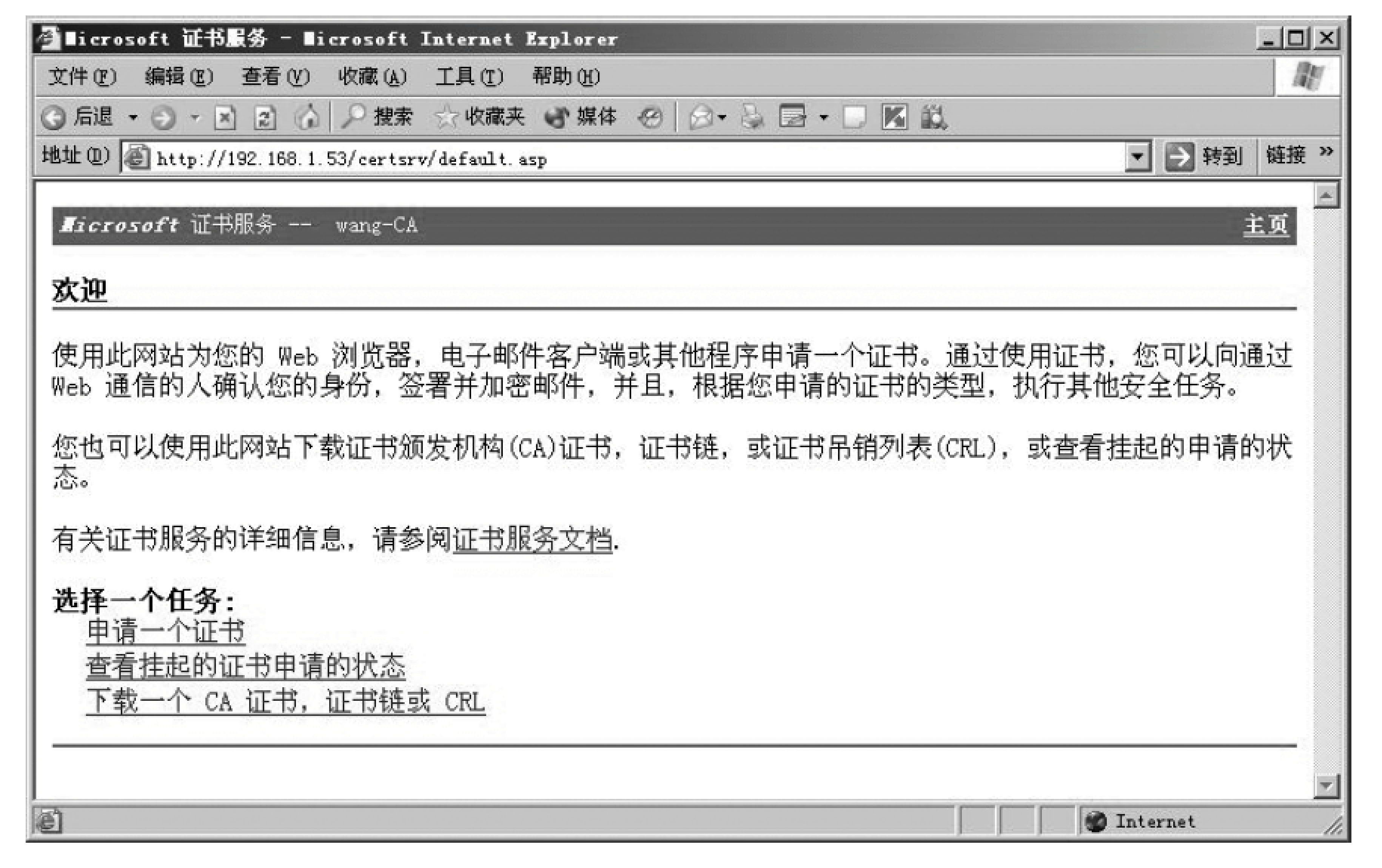


图 8-57　证书申请网页首页

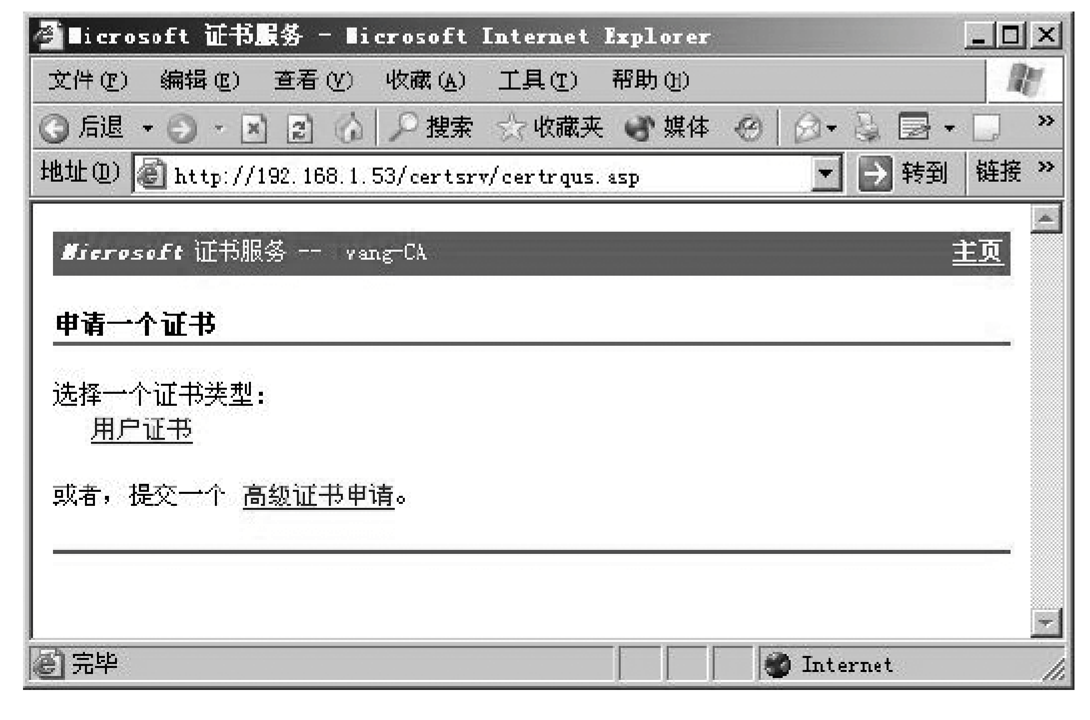


图 8-58　【申请一个证书】页面

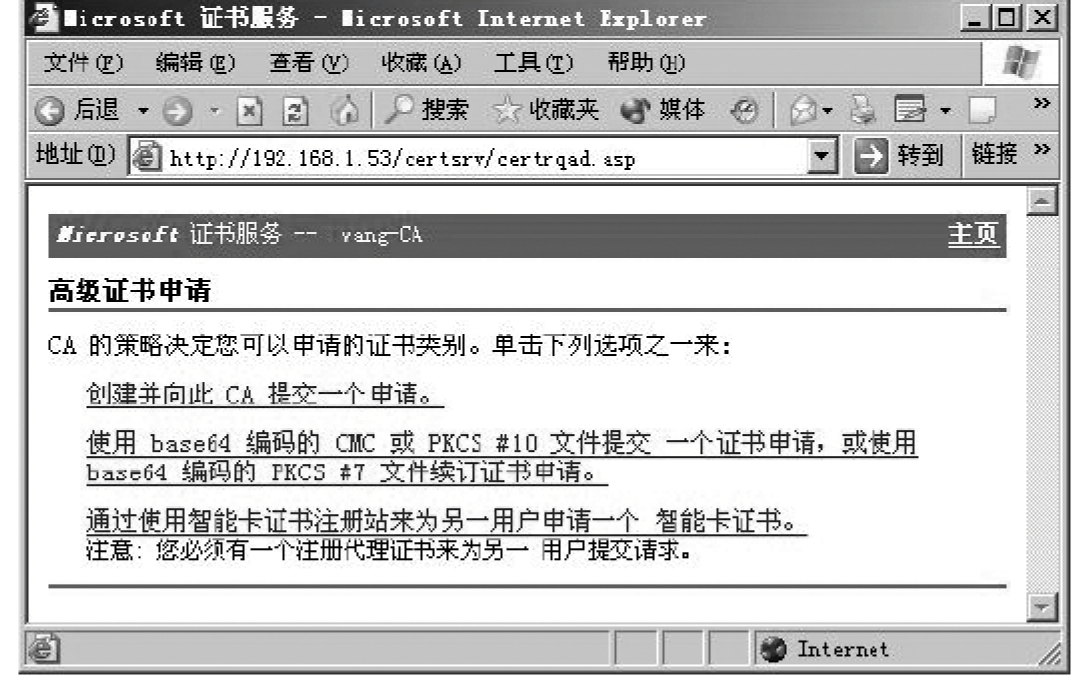


图 8-59　【高级证书申请】页面（一）



⑤ 单击【创建并向此 CA 提交一个申请】链接，打开如图 8-60 所示的【高级证书申请】页面(二)。在【证书模板】下拉列表框中选择【EFS 故障恢复代理】选项。

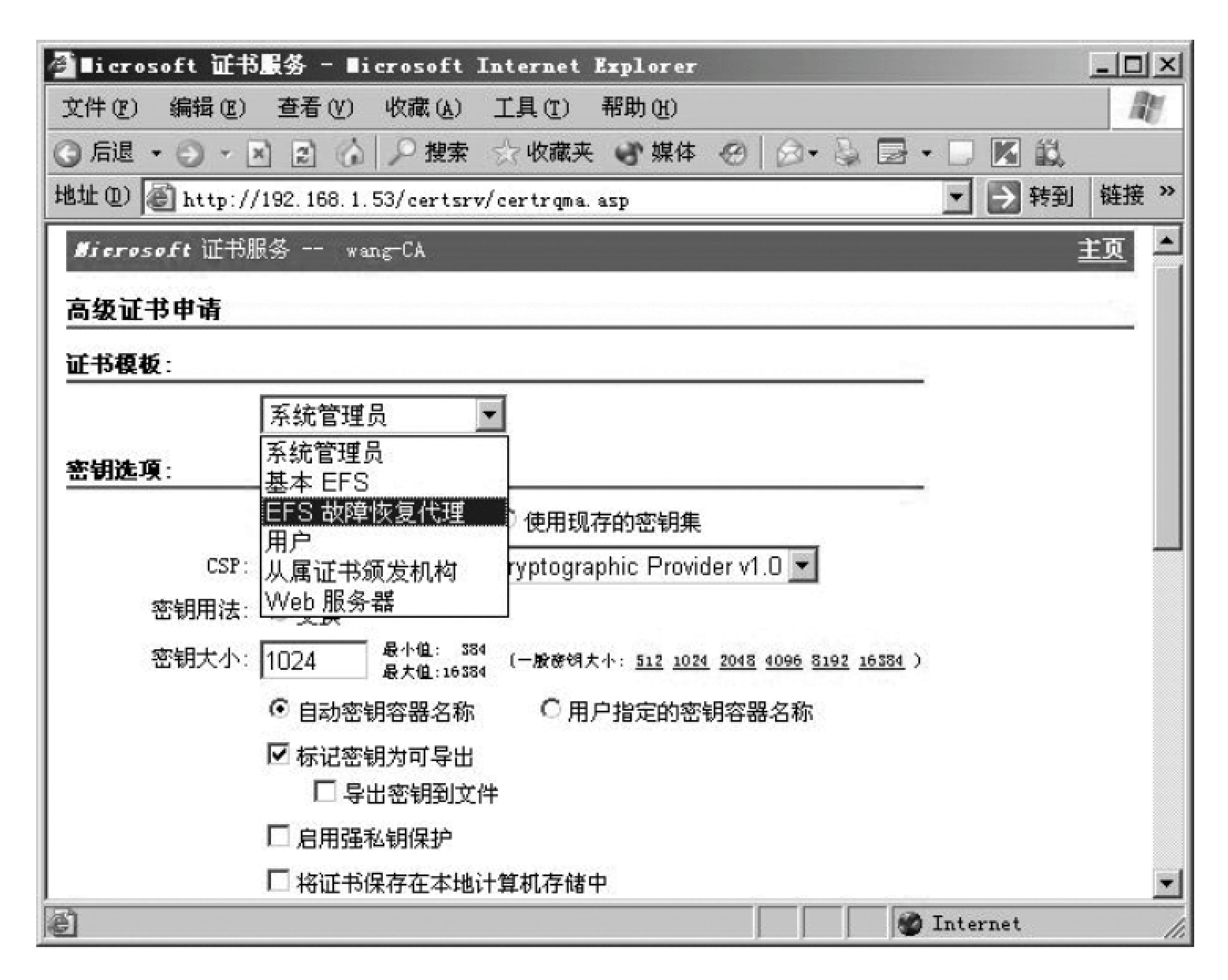


图 8-60 【高级证书申请】页面(二)

注意：如果没有进行前面的步骤(第 2 步：以 Administrator 账户登录系统，配置【EFS 故障恢复代理】证书模板，使 Sanny 账户具有使用该模板进行注册的权限)，那么非系统管理员账户进行证书申请时，此步所出现的下拉列表框中没有【EFS 故障恢复代理】选项。

在高级证书申请中可供用户选择的选项包括以下几项。

- 加密服务提供程序选项：加密服务提供程序的名称、密钥大小、散列算法(SHA/RSA、SHA/DSA、MD2、MD5)和密钥规格(交换或签名)。
- 密钥生成选项：创建新密钥集或使用现有密钥集、将密钥标记为可导出、启用强密钥保护以及使用本地计算机存储区来生成密钥。
- 其他选项：将申请保存到 PKCS #10 文件，或添加希望添加到证书的任何特定属性。并可配置证书名称。

注意：Netscape 客户端无法使用高级选项网页。

⑥ 配置好后，单击页面底部的【提交】按钮(图中未显示)，系统会弹出如图 8-61 所示的【潜在的脚本冲突】提示框。单击【是】按钮，打开如图 8-62 所示的【证书已颁发】提示页面，提示要安装此证书。



图 8-61 【潜在的脚本冲突】提示框



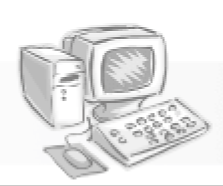




图 8-62 【证书已颁发】提示页面

⑦ 单击【安装此证书】链接，系统会弹出如图 8-63 所示的【潜在的脚本冲突】提示框。单击【是】按钮，开始安装新建的“EFS 故障恢复代理证书”，完成后出现如图 8-64 所示的【证书已安装】提示页面。此时整个“EFS 故障恢复代理证书”的申请就全部完成了。

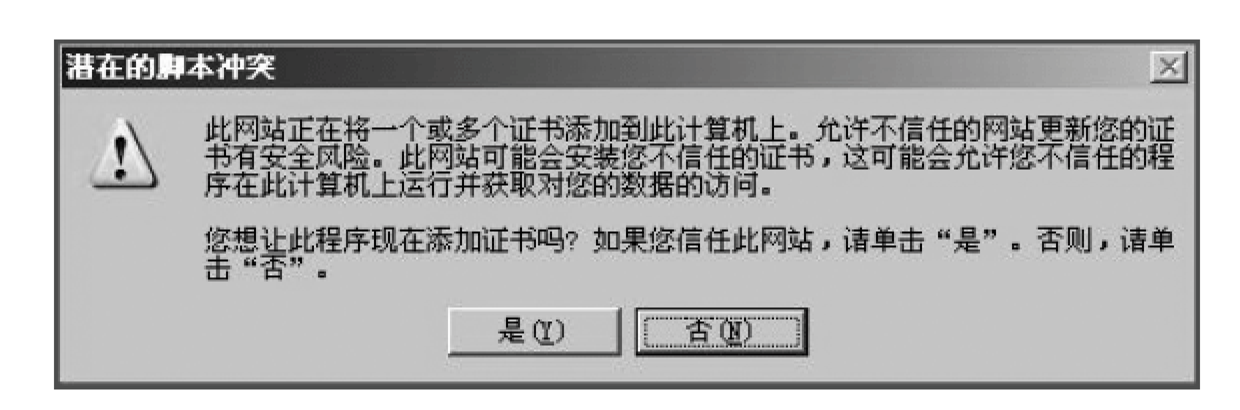


图 8-63 【潜在的脚本冲突】提示框



图 8-64 【证书已安装】提示页面

4. 配置故障恢复组策略

配置故障恢复组策略即添加域的故障恢复代理。创建了故障恢复代理证书后，要在域组策略中添加该证书。

该操作可在 Active Directory 内的任何站点、域或组织单位上执行。以证书文件形式添加故障恢复代理时，首先进行证书文件的导出，然后利用该证书文件创建 EFS 故障恢复代理。

> **注意**：域用户证书的导出可以由系统管理员和证书持有人来执行，都是在如图 8-65 所示的证书控制台中进行。如果是系统管理员，则可以查看和导出域用户所有的个人证书，如图 8-65 所示。





图 8-65 系统管理员可在【证书】控制台中查看和导出域用户所有的个人证书

以 Administrator 账户登录域控制器，具体操作步骤如下。

(1) 打开如图 8-65 所示的个人证书详细列表，在新创建的 EFS 故障恢复代理证书上右击，如图 8-66 所示，选择【导出】命令，打开如图 8-67 所示的【欢迎使用证书导出向导】对话框。



图 8-66 在【证书】控制台中选择【导出】命令



图 8-67 【欢迎使用证书导出向导】对话框





(2) 单击【下一步】按钮，打开如图 8-68 所示的【导出私钥】对话框。在此可选择是否导出私钥。由于在组策略中添加 EFS 故障恢复代理时一定要用.cer 格式的证书文件，所以必须经过下一步骤，将格式选择为.cer 再导出。在此只能选择【不，不要导出私钥】单选按钮。

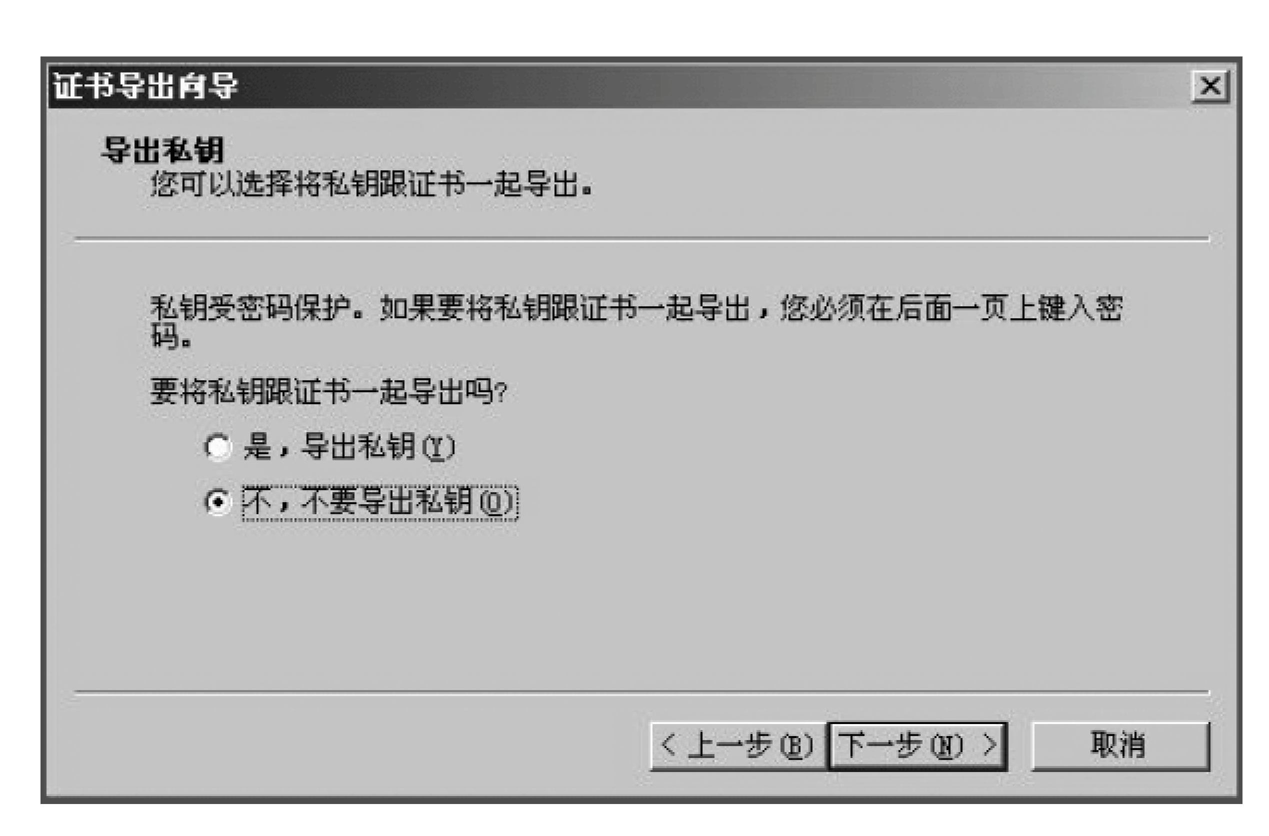


图 8-68　【导出私钥】对话框

(3) 单击【下一步】按钮，打开如图 8-69 所示的【导出文件格式】对话框。

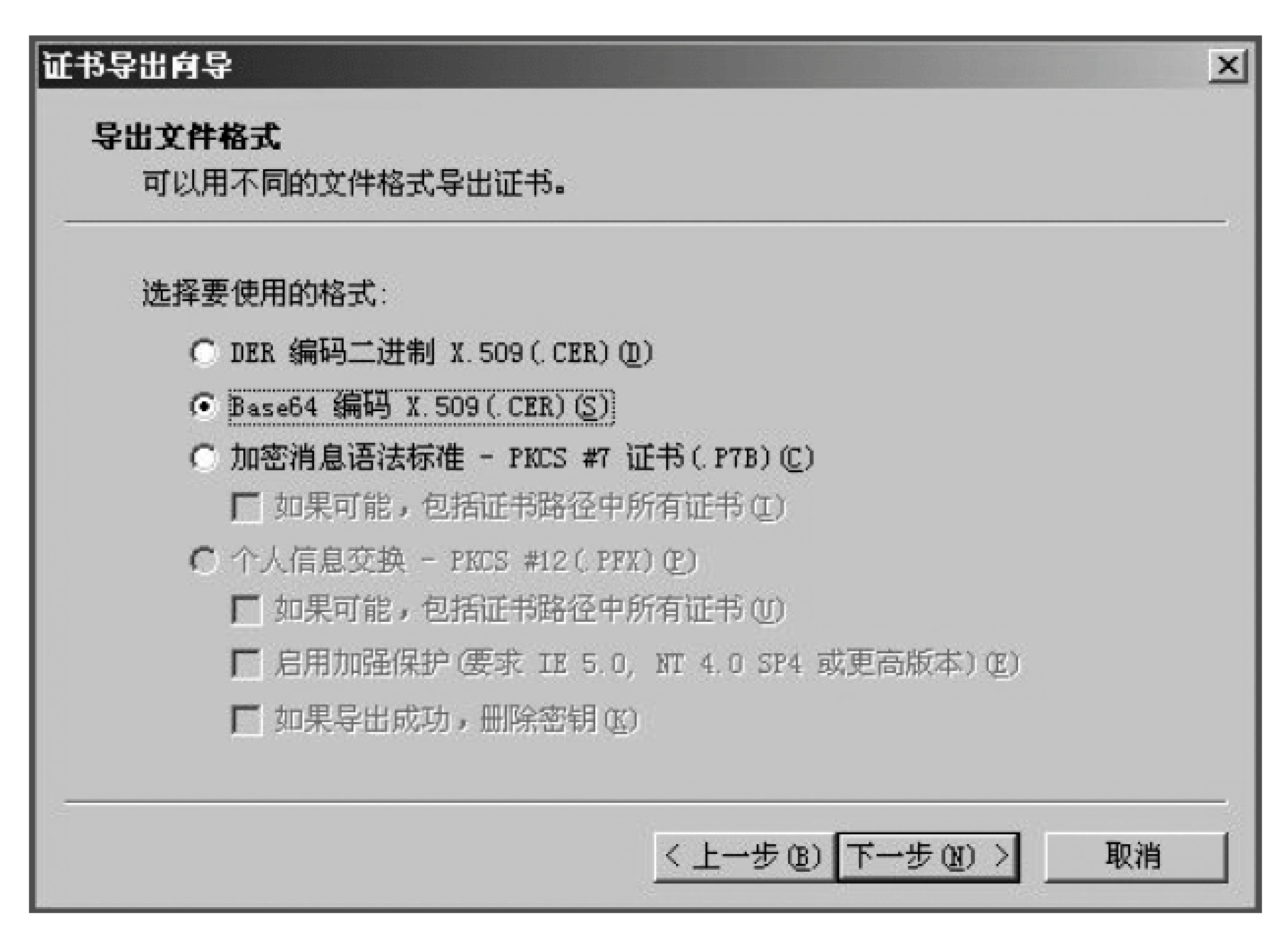


图 8-69　【导出文件格式】对话框

注意：如果在如图 8-68 所示的对话框中选择【是，导出私钥】单选按钮，则打开如图 8-70 所示的【导出文件格式】对话框，在其中就不能选择.cer 格式的证书文件了。

(4) 在如图 8-70 所示的对话框中选中【Base64 编码 X.509(CER)】单选按钮，单击【下一步】按钮，打开如图 8-71 所示的【要导出的文件】对话框。在其中的【文件名】文本框中输入证书文件名。默认存放的路径是 Documents and Settings 文件夹下相应用户账户的文件夹下，也可通过单击【浏览】按钮更改证书文件存放位置。

(5) 单击【下一步】按钮，打开如图 8-72 所示的【正在完成证书导出向导】对话框。在文本框中显示了导出的证书文件的配置摘要(如果觉得某项配置不正确，可以通过单击【上一步】按钮返回到相应步骤重新配置)。单击【完成】按钮开始导出证书文件，导出成功后系统会弹出一个【导出成功】提示框。



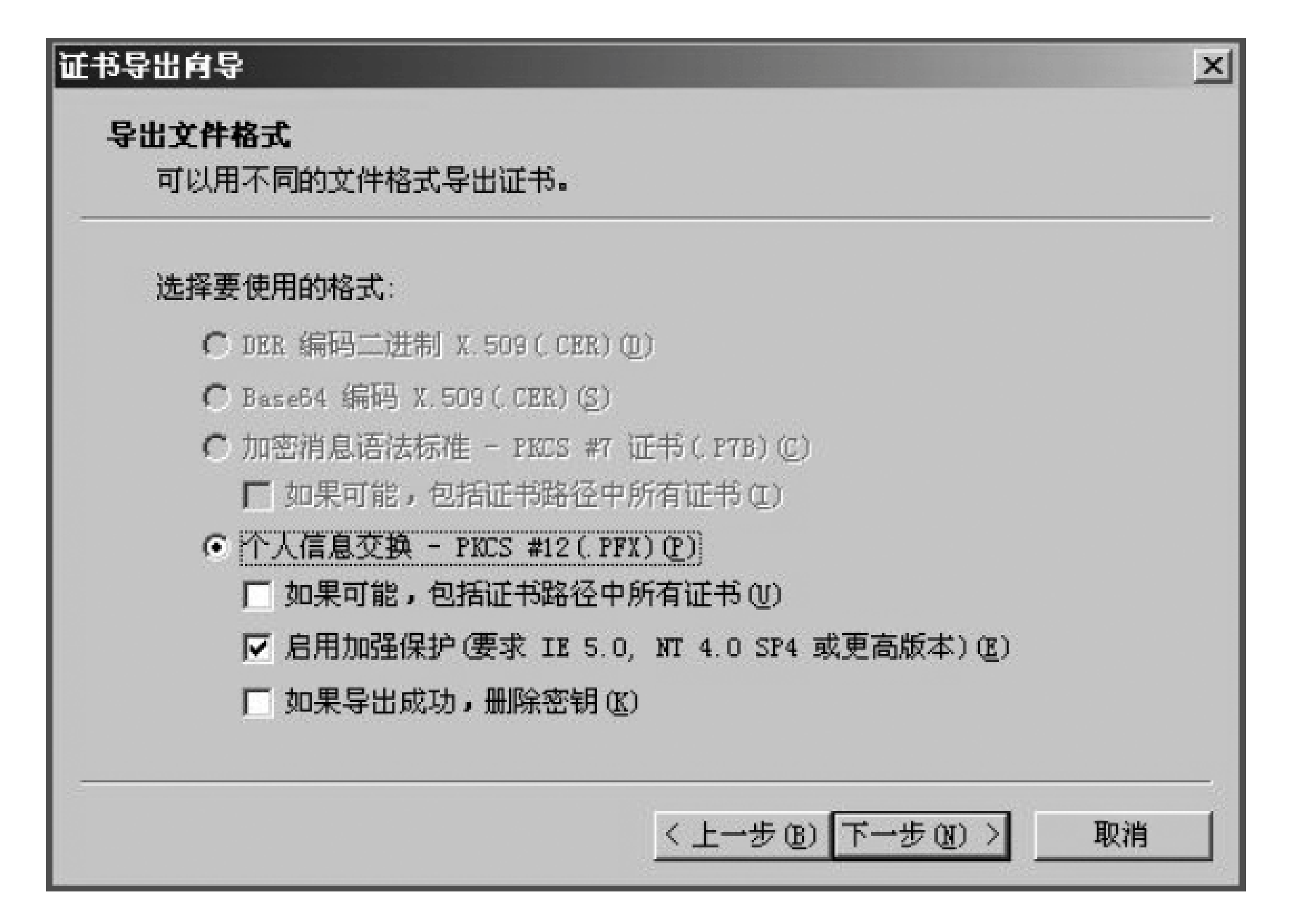


图 8-70 【导出文件格式】对话框



图 8-71 【要导出的文件】对话框

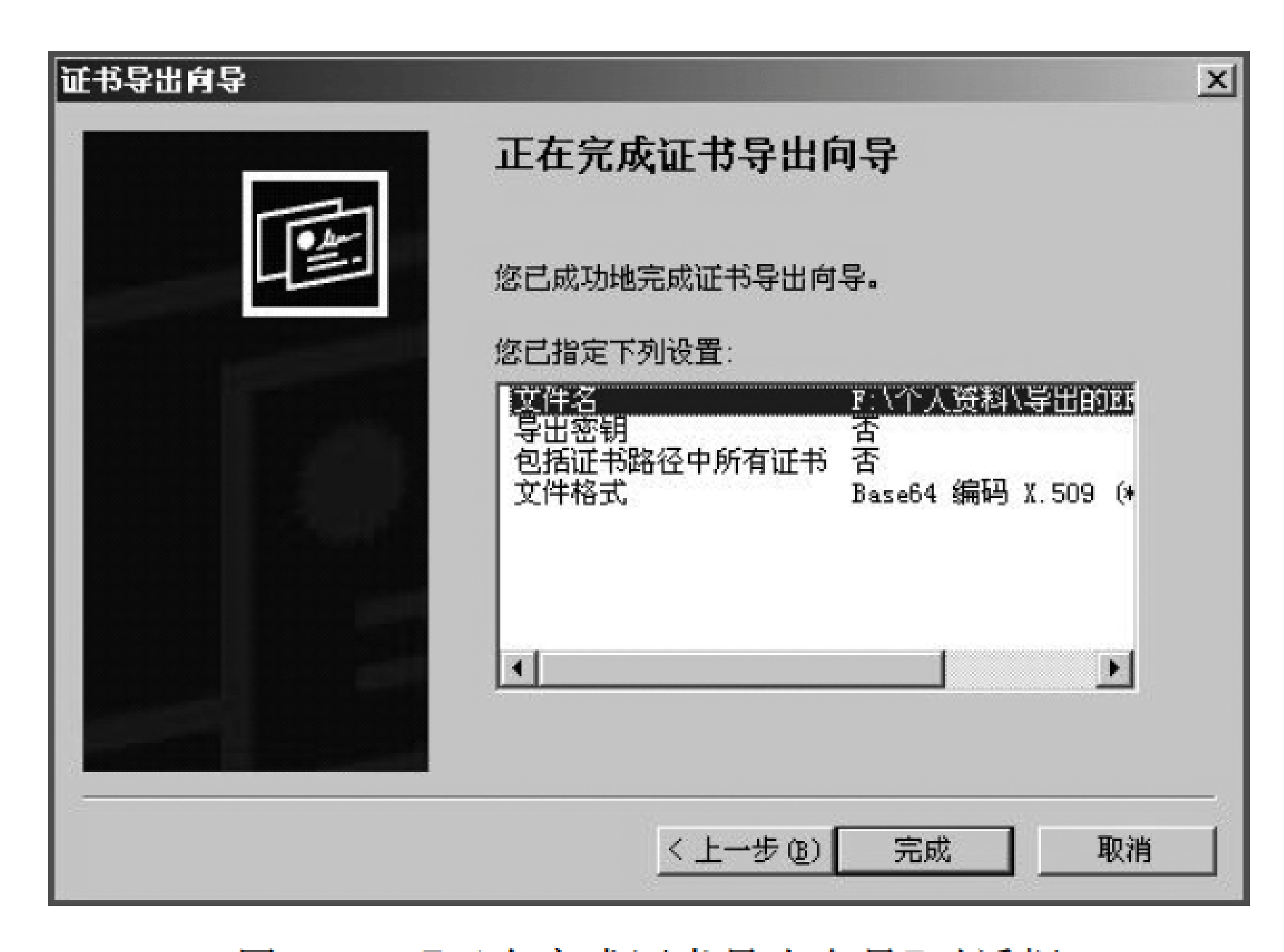


图 8-72 【正在完成证书导出向导】对话框





证书导出后，接下来就要利用这个证书文件创建 EFS 故障恢复代理了。

(6) 选择【开始】/【管理工具】/【Active Directory 用户和计算机】命令，打开【Active Directory 用户和计算机】对话框，如图 8-73 所示。



图 8-73　【Active Directory 用户和计算机】对话框

(7) 在要更改恢复策略的域上右击，在弹出的快捷菜单中选择【属性】命令，在打开的【域属性】对话框中选择【组策略】选项卡，如图 8-74所示。



图 8-74　【域属性】对话框的【组策略】选项卡

(8) 如果原先在组策略中添加了新的组策略(系统默认有一个组策略选项)，则可在列表中选择要更改的组策略选项(在此以系统默认的组策略选项为例)，然后单击【编辑】按钮。

(9) 在打开的【组策略编辑器】中选择【计算机配置】/【Windows 设置】/【安全设置】/【公钥策略】命令，如图 8-75 所示。

(10) 在右侧详细信息列表窗格的【加密文件系统】选项上右击，如图 8-76 所示，选择【添加数据恢复代理程序】命令，打开如图 8-77 所示的【欢迎使用添加故障恢复代理向导】对话框。



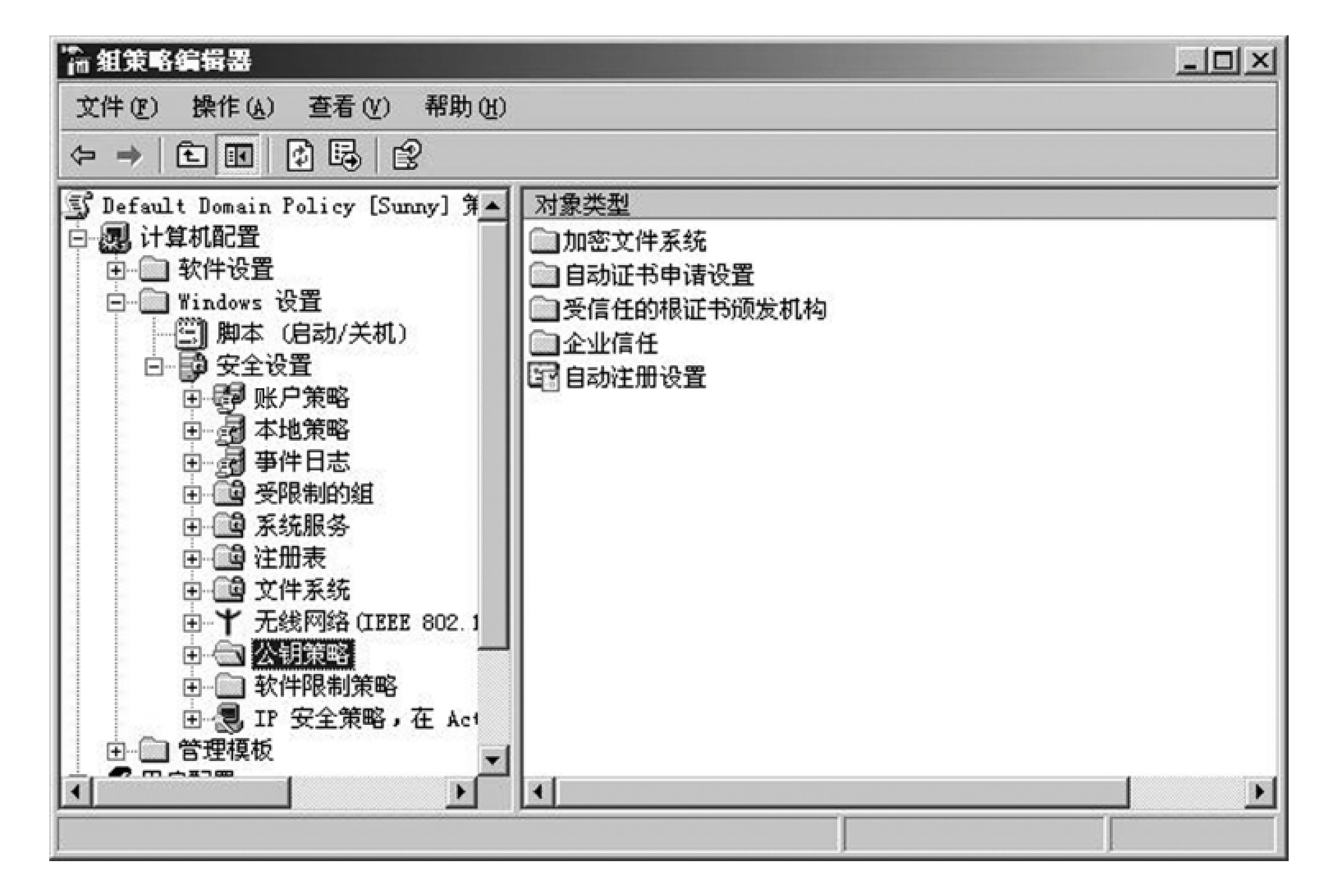


图 8-75　选择【组策略编辑器】中的【公钥策略】命令

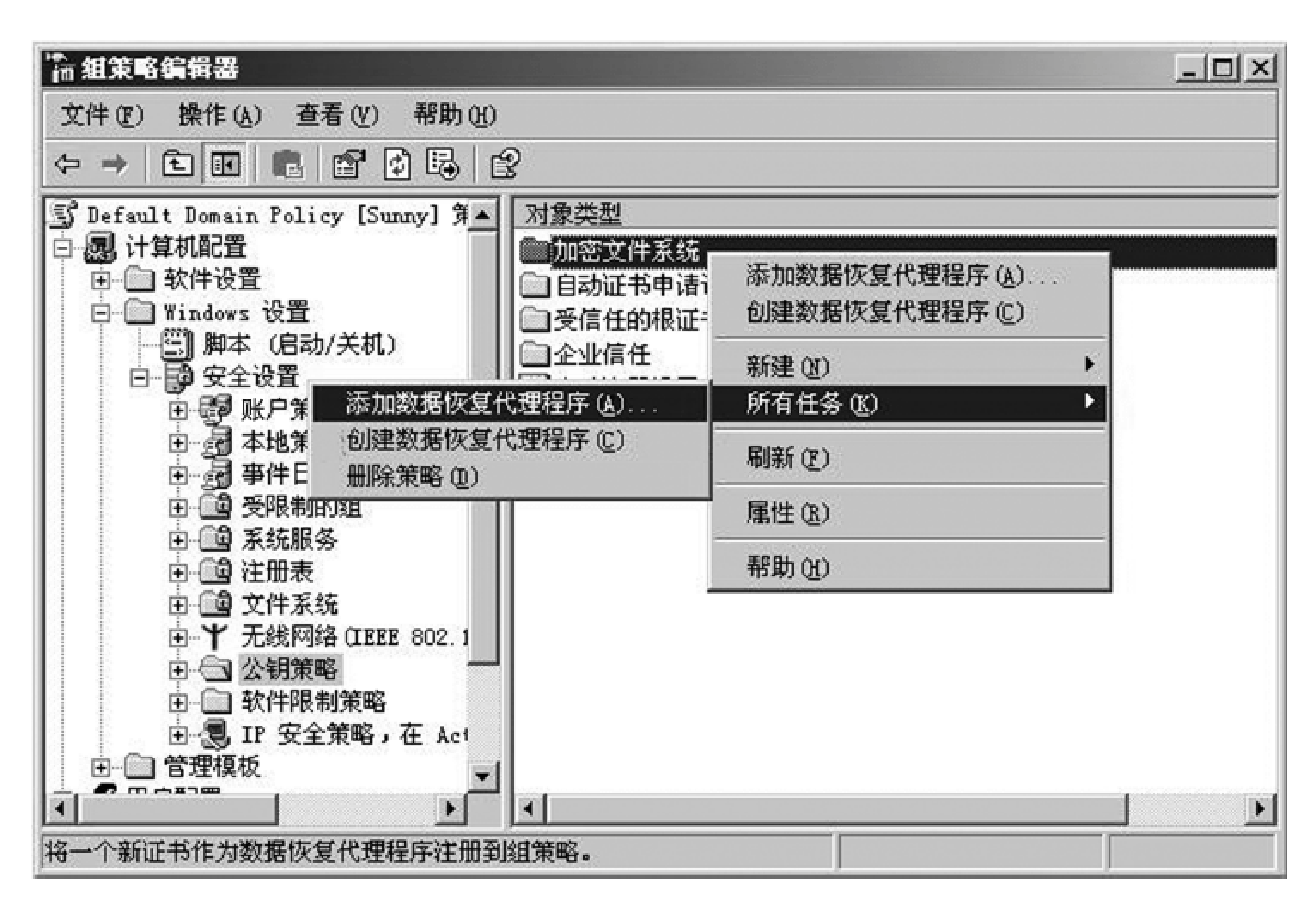


图 8-76　选择【添加数据恢复代理程序】命令

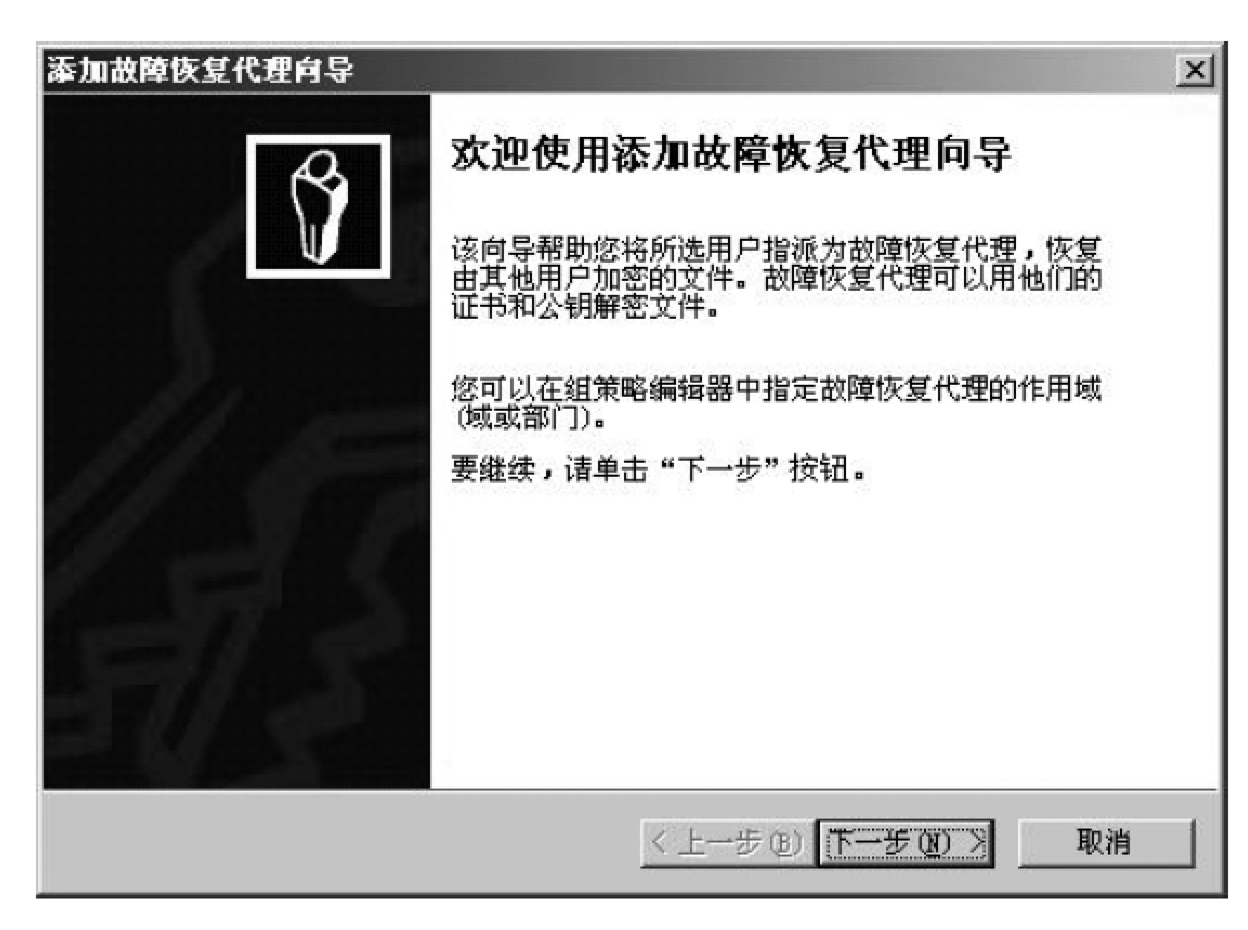


图 8-77　【欢迎使用添加故障恢复代理向导】对话框



注意：如果需要创建用户证书以用做“加密文件系统(EFS)”故障恢复代理证书，则在弹出的快捷菜单中选择【创建数据恢复代理程序】命令。

如果要使用现有的证书，则在弹出的快捷菜单中选择【添加数据恢复代理程序】命令，并按照向导所提供的说明来完成此过程。

如果要删除此EFS策略和每一个恢复代理，在弹出的快捷菜单中选择【删除策略】命令。如果选择该命令，用户仍然可以加密计算机上的文件(除非计算机上有EFS策略，否则不显示该命令)。

(11) 单击【下一步】按钮，打开如图8-78所示的【选择故障恢复代理】对话框。在这里要选择用于故障恢复代理的用户账户，只有创建了EFS故障恢复代理证书的用户才可以被指派。

(12) 单击【浏览文件夹】按钮，在打开的【打开】对话框中找到前面用来存放EFS故障代理证书文件的路径，并选择相应的证书文件，只能是.cer格式的，如图8-79所示。选择好后单击【打开】按钮，返回到如图8-78所示的对话框，不过此时已添加了故障恢复代理，以USER_UNKNOWN显示，如图8-80所示。

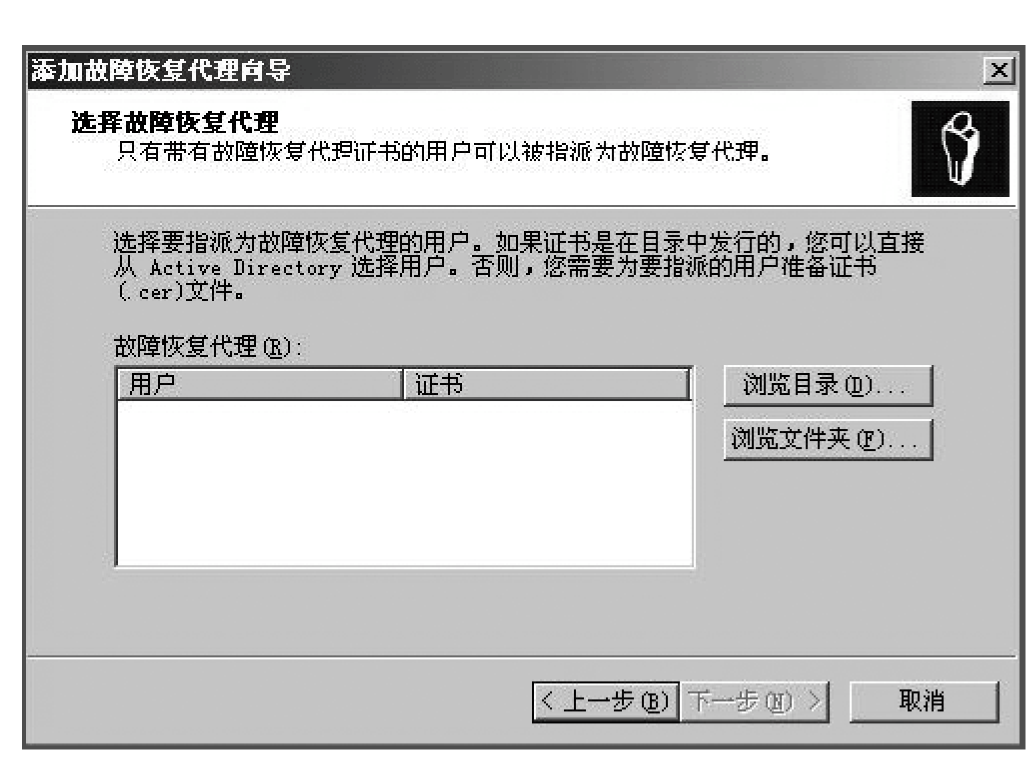


图8-78　【选择故障恢复代理】对话框



图8-79　在【打开】对话框中选择“证书文件”

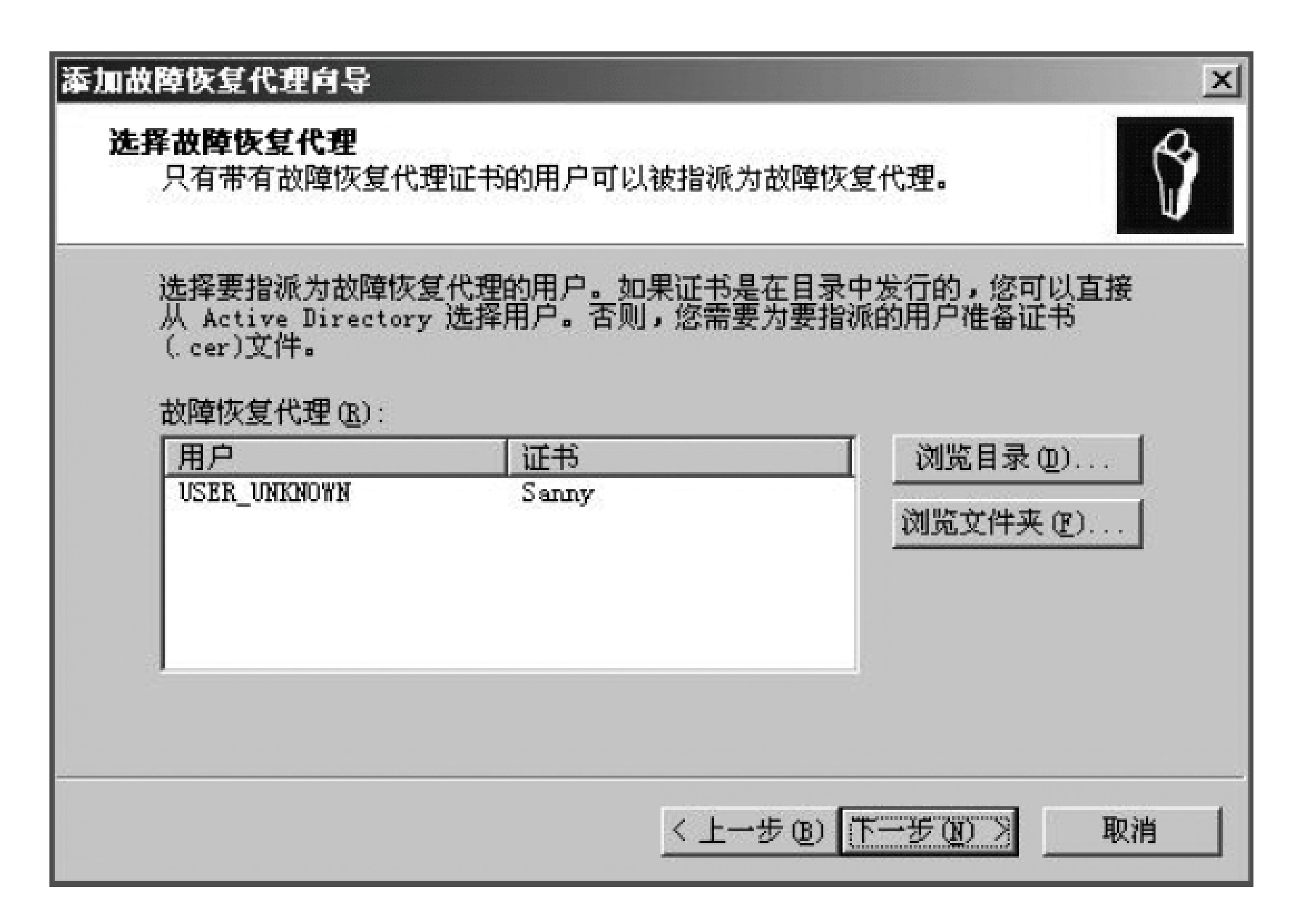


图8-80　【选择故障恢复代理】对话框

(13) 单击【下一步】按钮，打开如图8-81所示的【正在完成添加故障恢复代理向导】对



话框。单击【完成】按钮完成一个 EFS 恢复代理的指派。此时在【组策略编辑器】恢复中的【加密文件系统】选项右边的窗口中，可以看到新指派的 EFS 故障恢复代理，如图 8-82 所示。



图 8-81 【正在完成添加故障恢复代理向导】对话框

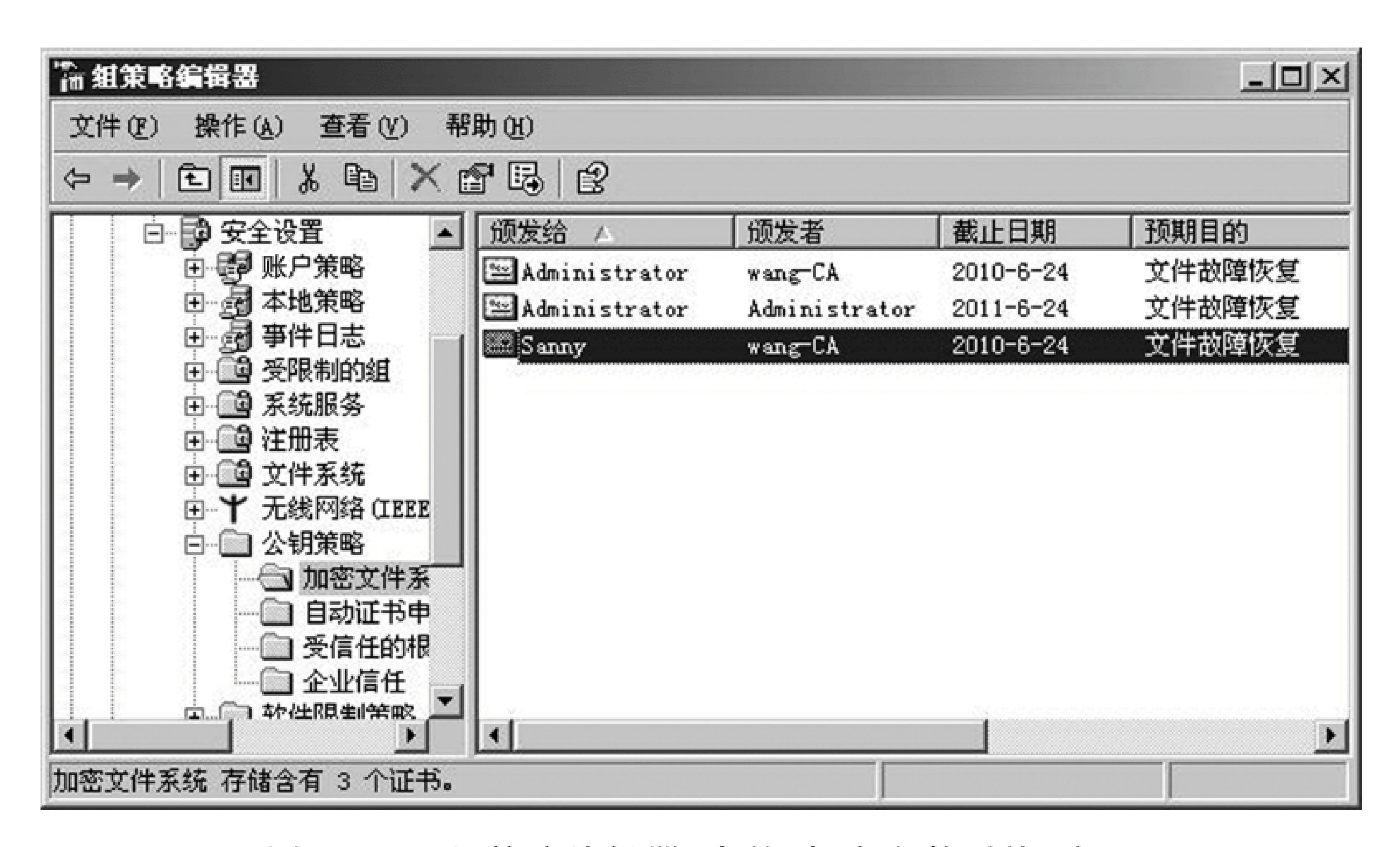


图 8-82 【组策略编辑器】中的【加密文件系统】窗口

通过以上四大步骤，完成了域的故障恢复代理的创建。如果我们想在没有证书颁发机构的情况下，创建独立计算机上的故障恢复代理，则进行如下操作。

5. 创建默认的独立计算机上的故障恢复代理

在独立计算机上默认没有故障恢复代理(在证书颁发机构不存在的情况下)，需要手动创建。以本地计算机的 Administator 身份登录到本地计算机上。

具体操作步骤如下：

(1) 在【运行】对话框中输入 cmd 命令，进入命令提示符下，在命令提示符窗口中输入 cipher. exe /r:dra 命令，然后按 Enter 键。



(2) 在出现提示时,输入密码来保护.PFX 文件,然后再次输入密码确认。按 Enter 键后即创建成功,如图 8-83 所示。



图 8-83　创建独立计算机默认恢复代理过程

(3) 关闭【命令提示符】窗口。

(4) 在控制台中打开【证书服务】控制台。查看一下系统管理员账户是否已有数据恢复证书,如果没有,则可在本地组策略编辑器窗口【公钥策略】的【加密文件系统】选项上右击,在弹出的快捷菜单中选择【添加数据恢复代理程序】命令(见图 8-76),即可创建一个 Administrator 账户用于恢复数据的证书。

(5) 在所创建的数据恢复证书上右击,在弹出的快捷菜单中选择【导出】命令(见图 8-66),把刚才所创建的证书导出在一个位置保存。注意一定以 X.509 文件格式导出,否则该证书不能用于数据恢复。

(6) 再在组策略中的【加密文件系统】选项上右击,在弹出的快捷菜单中选择【添加数据恢复代理程序】命令,打开如图 8-77 所示的【欢迎使用添加故障恢复代理向导】对话框。随后的步骤就与前面介绍的向域中添加 EFS 故障恢复代理的方法一样,不再赘述。

8.5　密钥的存档与恢复

8.5.1　密钥的存档与恢复概述

密钥对于 PKI 来说是非常重要的,特别是其中的私钥,一旦遗失或泄露,数据的安全性将受到严重的威胁。而这类密钥的代码很长,几十位甚至几百位,一般人是无法记住的,因此,必须考虑密钥的安全性问题。解决方法是在系统中配置“密钥的存档和恢复”功能。

1. 密钥存档

为了降低私钥遭受攻击的机会,在默认情况下,证书的私钥不存档。如果要将密钥存档,需要进行配置。密钥存档后,受领人向 CA 提供其私钥,CA 将该私钥存储在它的数据库中。

2. 密钥恢复

当密钥受领人意外丢失其私钥,或者管理员希望恢复特定受领人的密钥以便访问该密钥保护的数据时,可以使用密钥恢复得到存档的私钥。

密钥恢复过程需要管理员检索加密的证书和私钥,然后要求密钥恢复代理(KRA)将它们提交给 CA,通过提交正确签名的密钥恢复申请,申请者将获得受领人的证书和私钥。申请者在必要时可以使用该密钥,或将其传送给受领人继续使用。

注意: 只有在运行企业 CA 的 Windows Server 2003 Enterprise Edition 和 Windows Server 2003 Datacenter Edition 上,密钥存档和密钥恢复功能才可用。



8.5.2 密钥的存档和恢复步骤

使用 Microsoft 证书颁发机构进行密钥的存档和恢复需要执行如图 8-84 所示步骤。

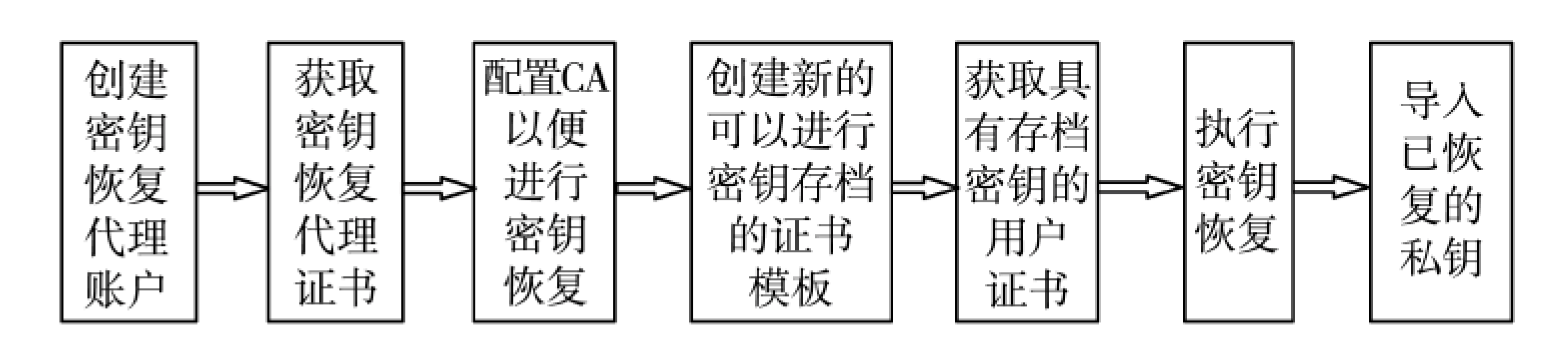


图 8-84 密钥的存档和恢复步骤

上述步骤(1)～(5)完成密钥的存档配置。当私钥丢失，通过步骤(6)和步骤(7)进行密钥的恢复。

1. 创建密钥恢复代理账户

配置并添加密钥恢复代理证书模板，使之成为可以由企业 CA 颁发的模板。

具体操作步骤如下：

(1) 以 Administrator 账户登录域控制器（建议采用 Windows Server 2003 R2 EnterPrise Edition)，在【运行】对话框中输入 certtmpl. msc 命令，打开如图 8-32 所示的【证书模板】控制台窗口。

(2) 双击【密钥恢复代理】选项，在打开的【属性】对话框中选择【安全】选项卡，如图 8-85 所示。在默认情况下，可以注册密钥恢复代理证书模板的安全组是 Domain Administrators 和 Enterprise Administrators 组成员。如果需要添加另一个恢复代理，则单击【添加】按钮以添加用户，并授予该用户“读取”和“注册”权限。

(3) 在如图 8-85 所示的对话框中选择【颁发要求】选项卡，如图 8-86 所示。取消选中【CA 证书管理程序批准】复选框，然后单击【确定】按钮，关闭【证书模板】窗口。

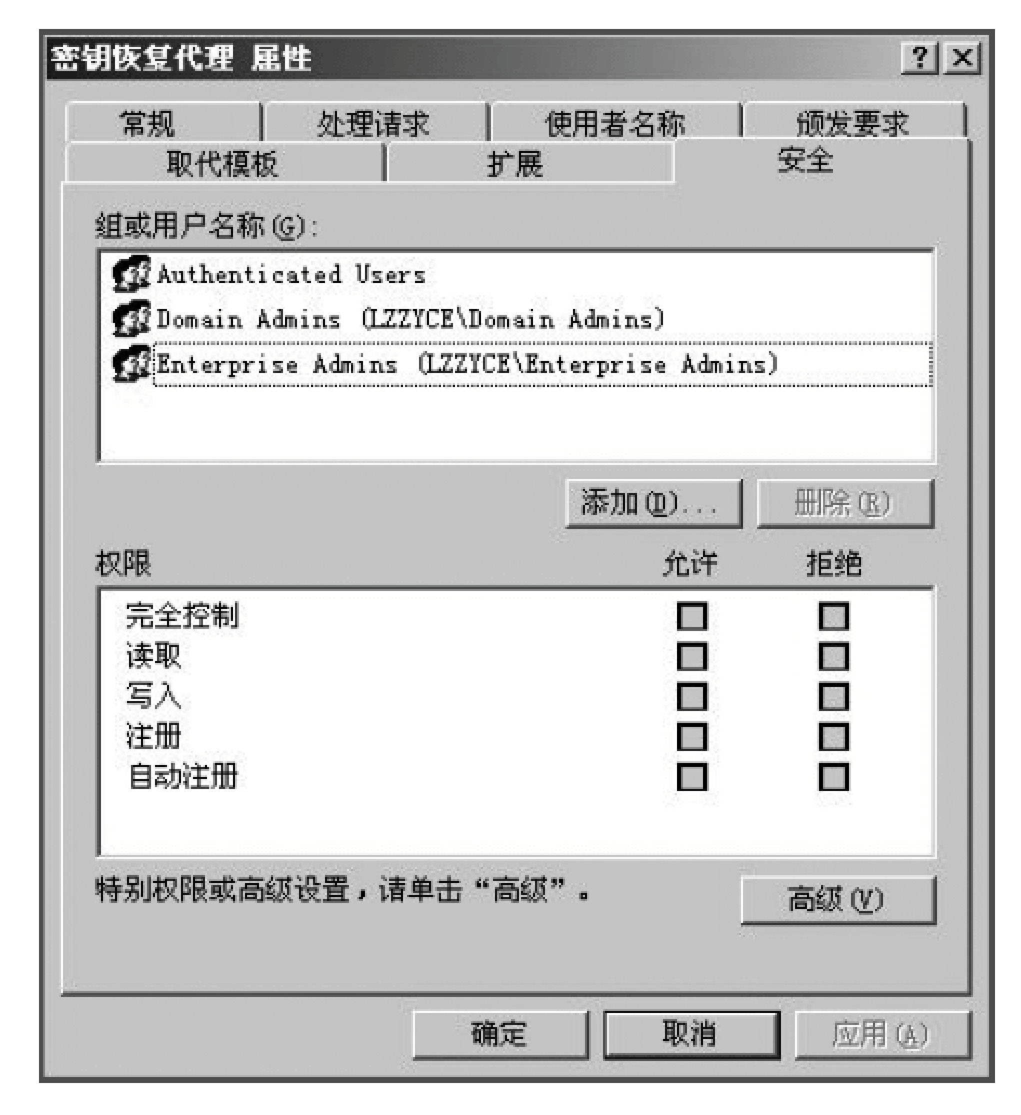




图 8-85 【密钥恢复代理 属性】对话框的【安全】选项卡

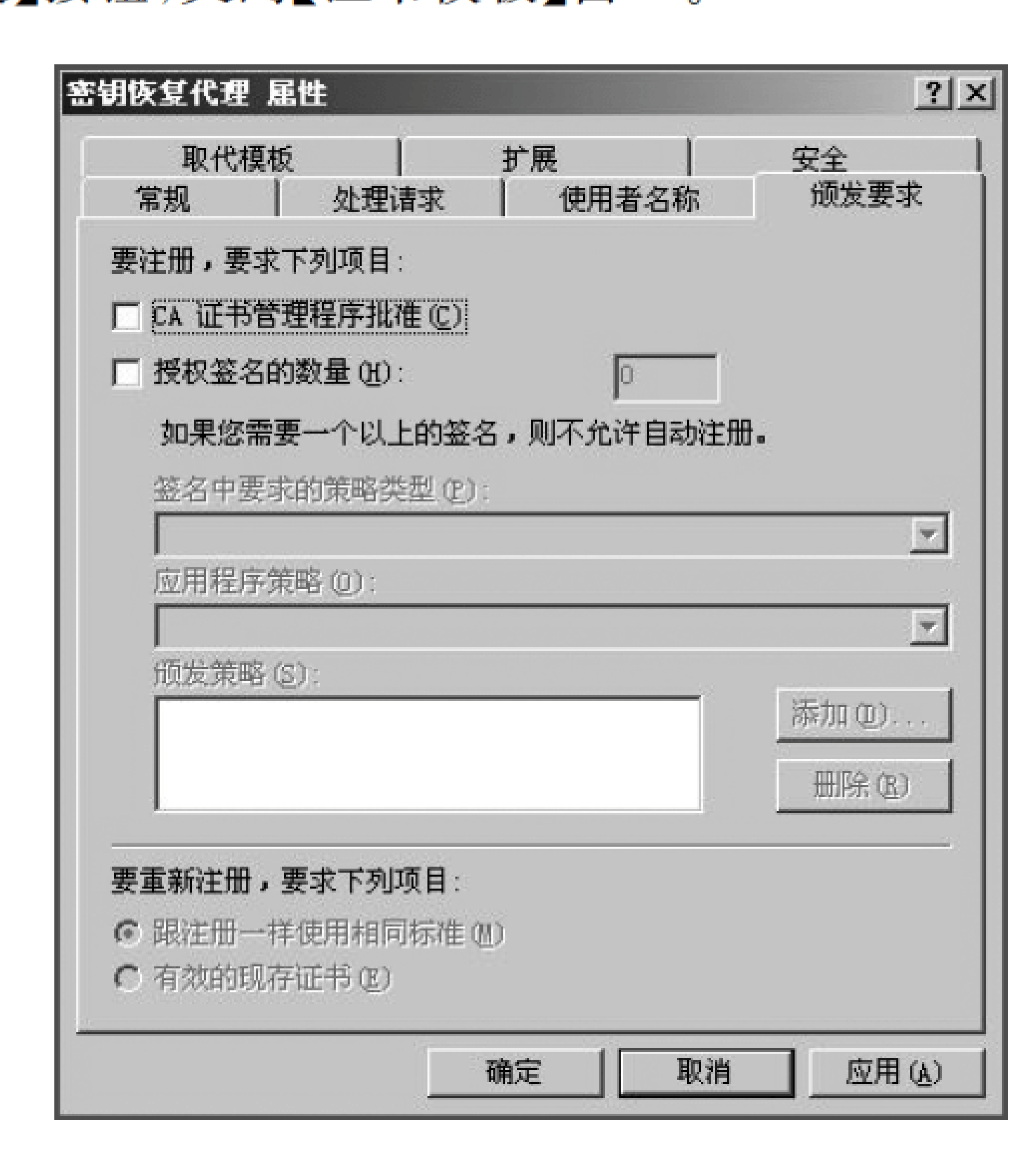


图 8-86 【颁发要求】选项卡



(4) 选择【开始】/【管理工具】/【证书颁发机构】命令，打开如图 8-87 所示【证书颁发机构】控制台窗口。



图 8-87　【证书颁发机构】控制台窗口

(5) 在左侧窗口的目录树中，右击【证书模板】选项，在弹出的快捷菜单中选择【新建】/【要颁发的证书模板】命令，打开如图 8-88 所示的【启用证书模板】对话框。选择【密钥恢复代理】选项，单击【确定】按钮即可。

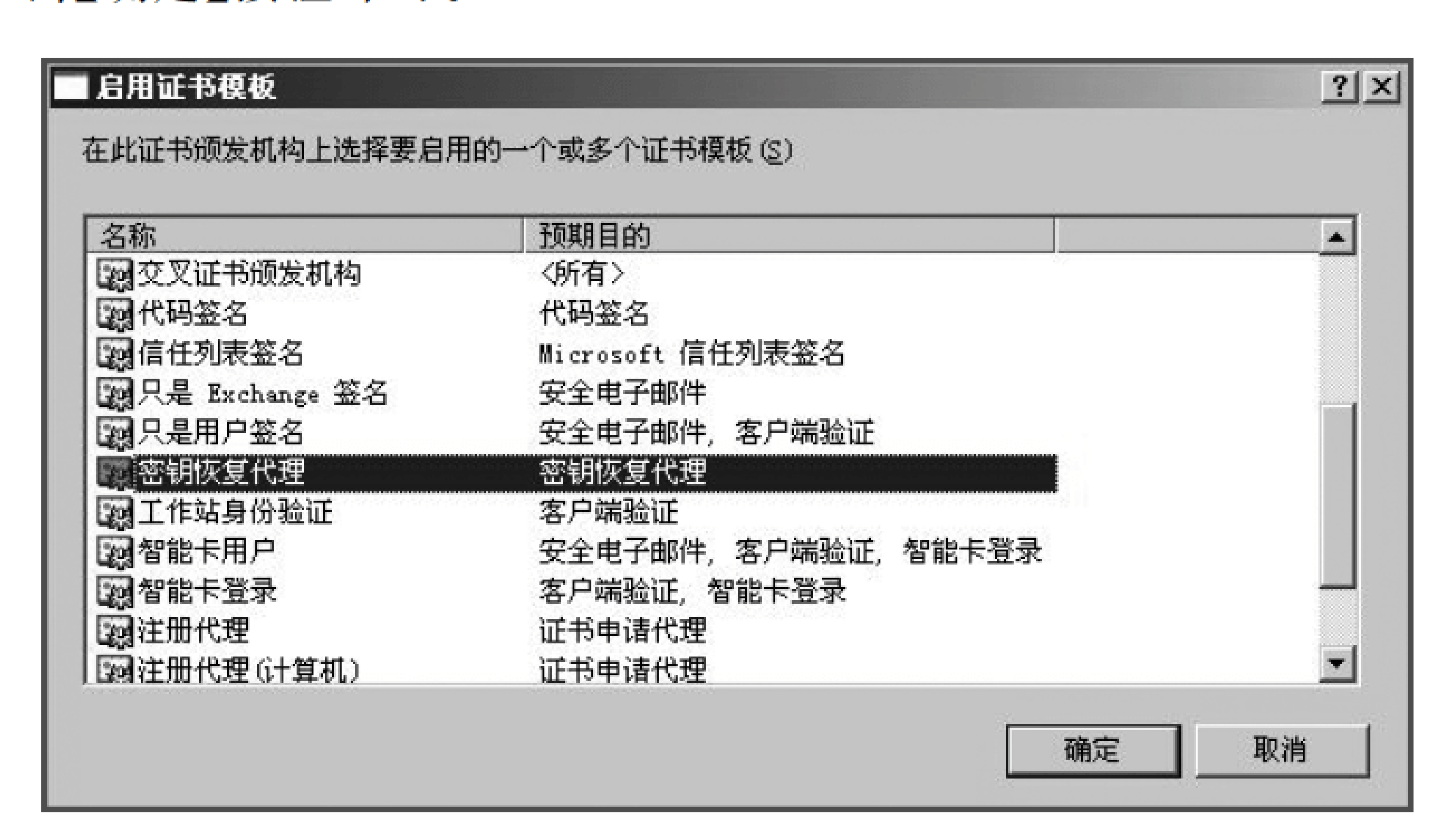


图 8-88　【启用证书模板】对话框

2. 获取密钥恢复代理证书

此步骤将获取用于恢复私钥的密钥恢复代理证书。以 Sanny 账户登录域控制器，具体操作步骤类似申请“EFS 故障恢复代理”证书(在此不再详述)。这里以网页的形式进行申请，如图 8-89 所示。申请成功后可以从控制台的【证书】窗口中看到安装成功列表，如图 8-90 所示。

3. 配置 CA 以便进行密钥恢复

因为密钥是与对应的证书颁发机构和证书模板息息相关的，所以要使私钥可存档和可进行密钥恢复，就需要在相应的证书颁发机构和证书模板上启用这一属性，即配置企业 CA 以使用上一个步骤获取的密钥恢复代理证书。

具体配置步骤如下：

(1) 首先要在证书颁发机构上启用密钥存档和恢复属性。选择【开始】/【管理工具】/【证书颁发机构】命令，打开如图 8-87 所示【证书颁发机构】控制台窗口。



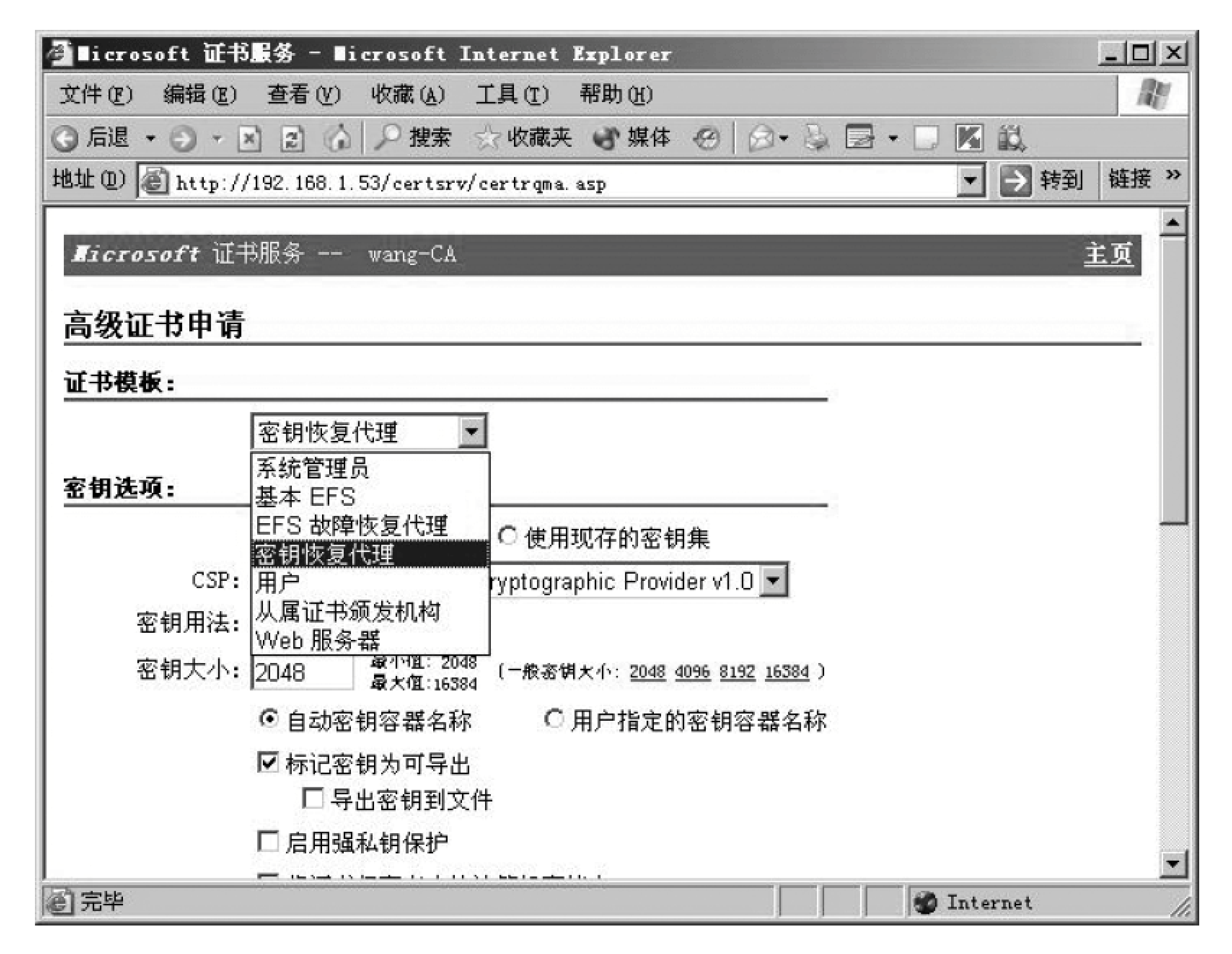


图 8-89 【高级证书申请】页面



图 8-90 从控制台的【证书】窗口中看到安装成功列表

(2) 在左边窗格中选择下面的证书颁发服务器，右击并在弹出的快捷菜单中选择【属性】命令，在打开的【证书颁发机构 属性】对话框中选择【故障恢复代理】选项卡，如图 8-91 所示。选择【存档密钥】单选按钮，在【要使用的故障恢复代理数目】文本框中，指定恢复存档的密钥所需的故障恢复代理的数目，然后将 8.4 节创建的故障恢复代理添加到【密钥故障恢复代理证书】列表中。

(3) 单击【确定】按钮，完成 CA 的密钥存档和恢复属性。接下来配置证书模板控制台中的证书模板。

(4) 在【运行】对话框中输入 certtmpl. msc 命令，打开【证书模板】控制台窗口，参见图 8-32。



（5）在右侧详细信息列表窗格中选择要配置密钥存档和恢复属性的证书模板（比如选择【EFS故障恢复代理-A】证书模板）上右击，在弹出的快捷菜单中选择【属性】命令。在打开的对话框中选择【处理请求】选项卡，如图8-92所示。选中【把使用者的加密私钥存档】复选框，单击【确定】按钮完成配置。

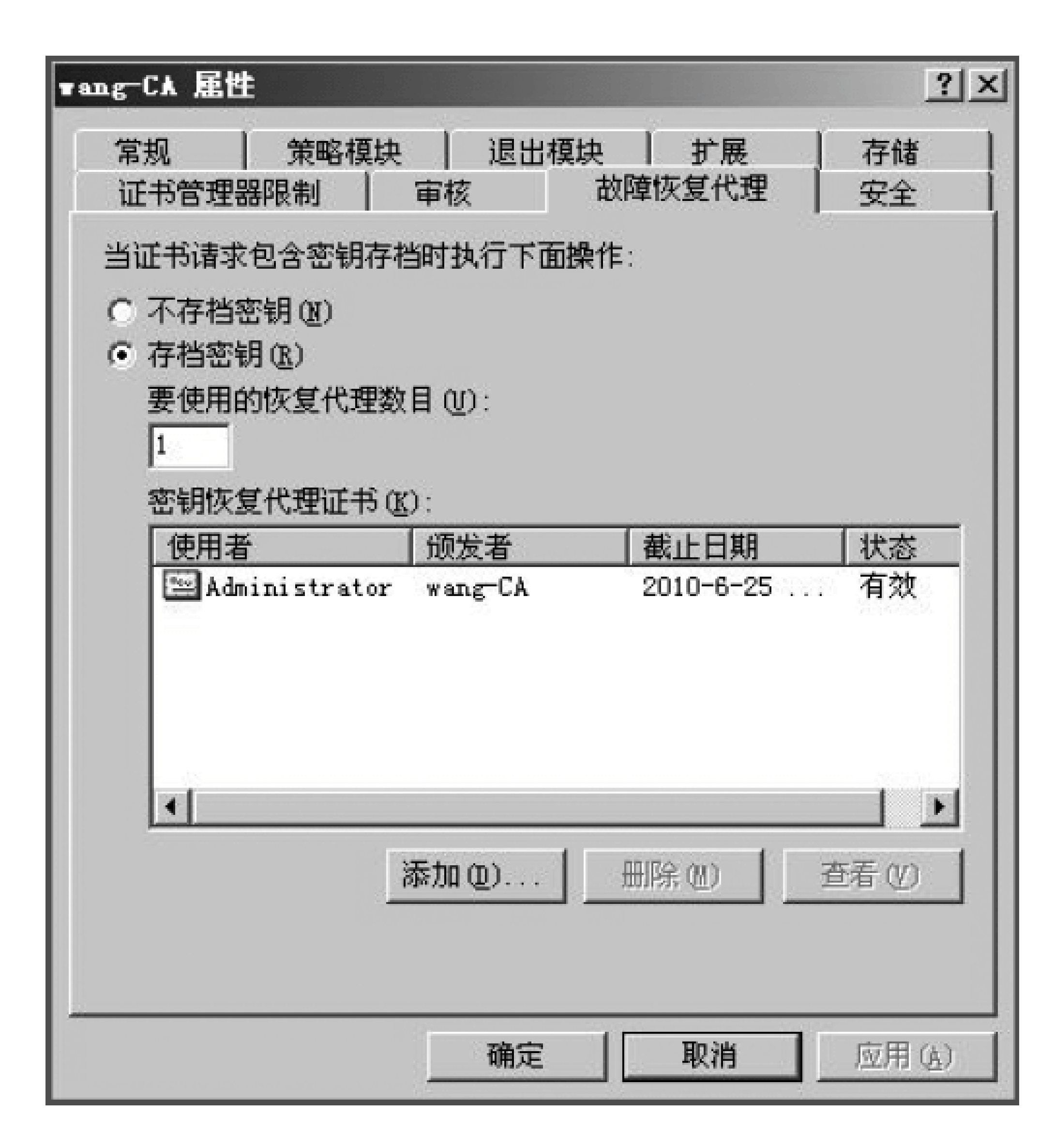


图 8-91　【证书颁发机构属性】对话框中的【故障恢复代理】选项卡

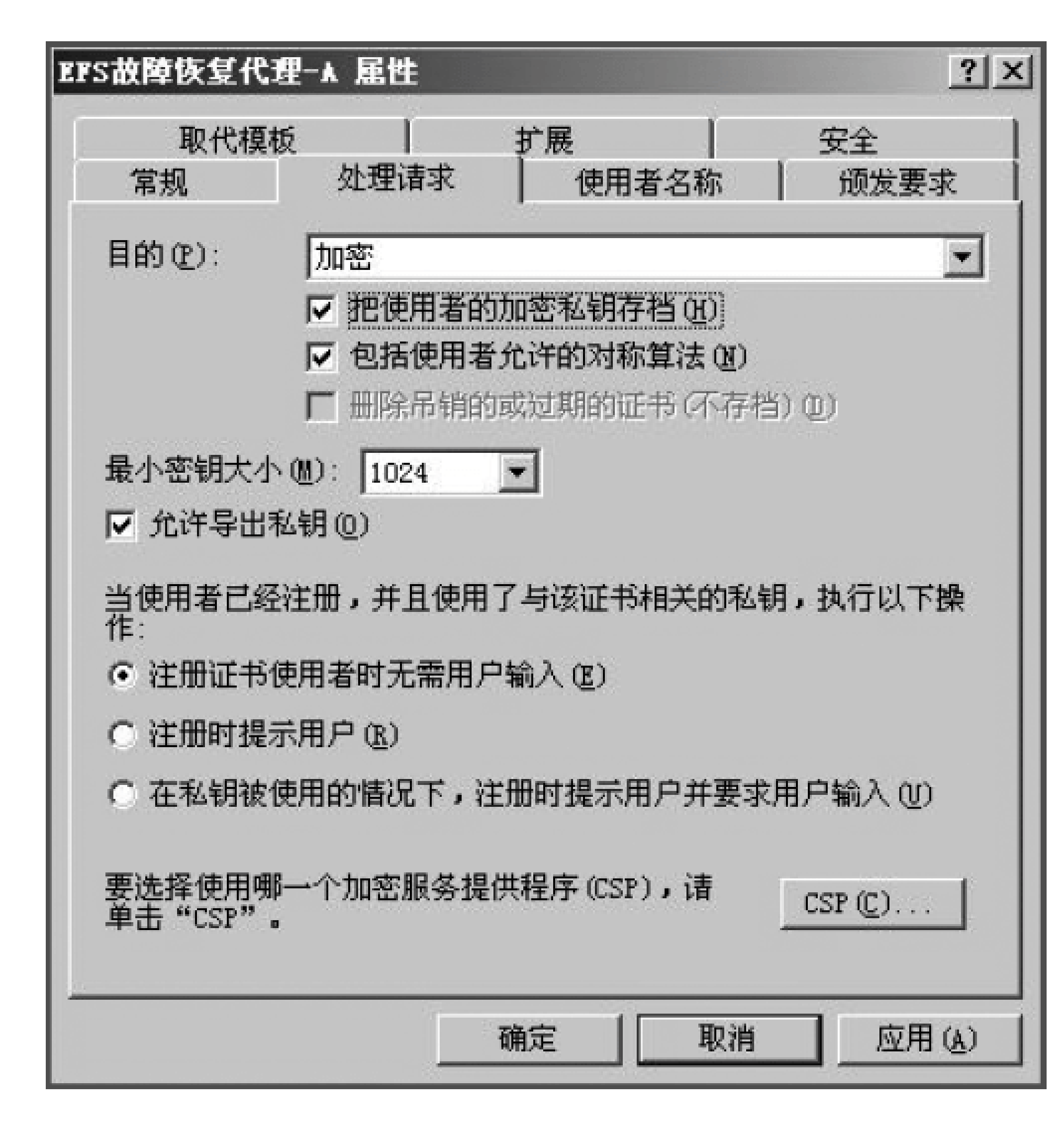


图8-92　【证书模板属性】对话框中的【处理请求】选项卡

注意：并不是在证书模板控制台中的所有证书模板都可以配置密钥存档和恢复属性的，在窗口中一些图标呈灰色的默认模板是没有【把使用者的加密私钥存档】复选项的，这样也就无法配置证书模板支持密钥存档。这些模板通常就是系统预配置的证书模板。

（6）按前面介绍的方法在控制台中添加【证书管理单元】，不过此时要添加的不是个人证书，而是计算机账户证书。在添加【证书管理单元】时，在如图8-93所示的【证书管理单元】

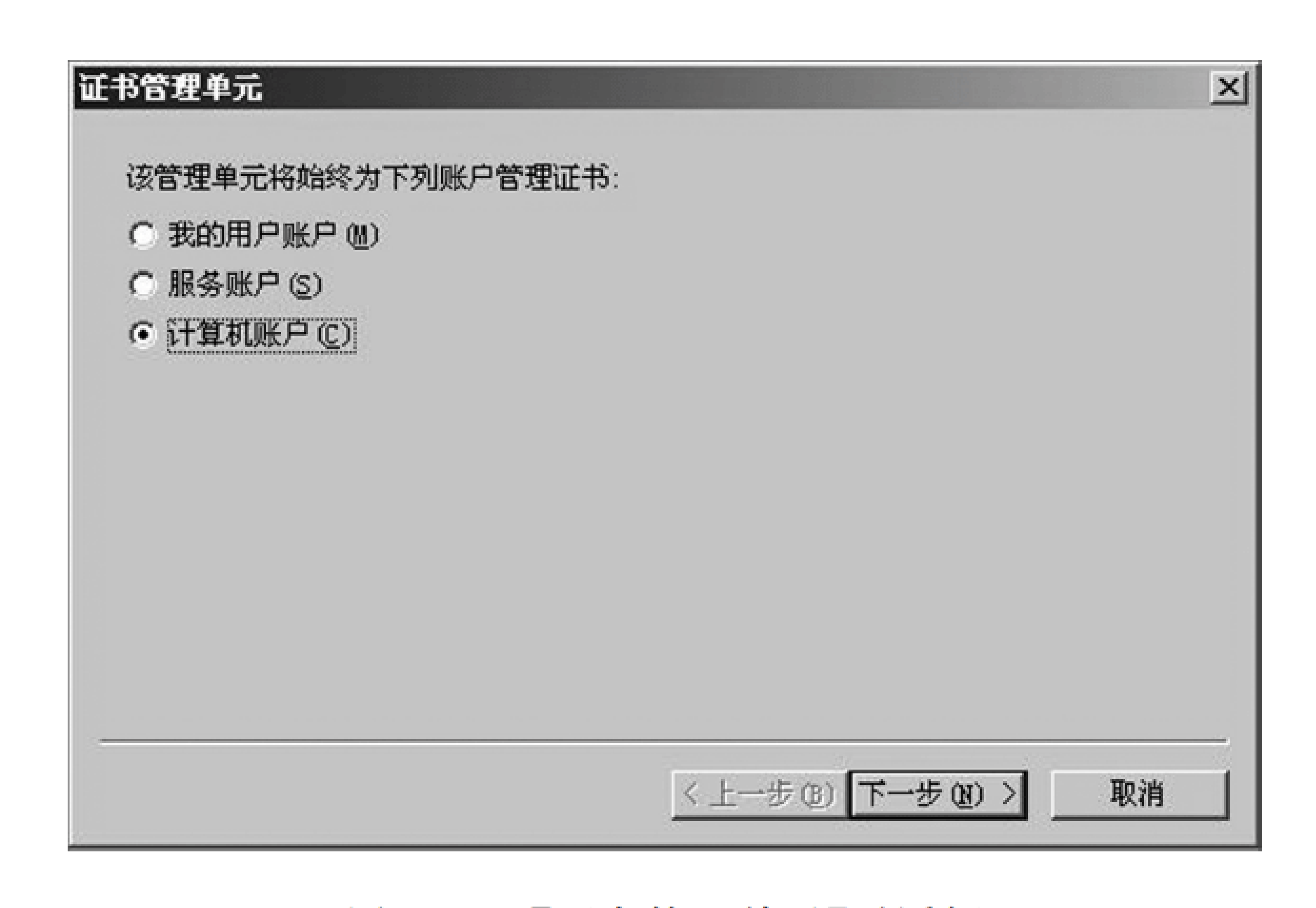


图 8-93　【证书管理单元】对话框



对话框中选择【计算机账户】单选按钮。然后单击【下一步】按钮，在打开的如图 8-94 所示的【选择计算机】对话框中选择【本地计算机】单选按钮，最后显示的是计算机账户【证书管理单元】控制台，如图 8-95 所示。



图 8-94 【选择计算机】对话框



图 8-95 计算机账户【证书管理单元】控制台

(7) 验证密钥恢复代理证书是否已经安装。在控制台树中，选择【控制台根节点】/【证书(本地计算机)】/KRA/【证书】命令，即可见到所创建的密钥恢复代理证书。证书的计划用途是密钥恢复代理，并且证书被颁发给管理员。

(8) 最后，可将控制台另存为“控制台 2”。

4. 创建新的可以进行密钥存档的证书模板

该步骤可以在客户端计算机上的私钥丢失或损坏的情况下在域中进行密钥恢复。

具体操作步骤如下：

(1) 以 Administrator 账户登录域控制器，按照上一个实验介绍的方法打开【证书模板】控制台窗口，参见图 8-32。

(2) 在【运行】对话框中输入 mmc，打开一个空的【控制台】窗口，参见图 8-40。



（3）选择【文件】/【添加/删除管理单元】命令，打开如图 8-41 所示的对话框。

（4）单击【添加】按钮，打开如图 8-42 所示的对话框。在其中双击选择【证书模板】选项，然后单击【关闭】按钮返回到如图 8-41 所示的对话框。再单击【确定】按钮返回到如图 8-40 所示【控制台】窗口，此时已添加了【证书模板】管理单元，如图 8-96 所示（可另存为“控制台 3”）。

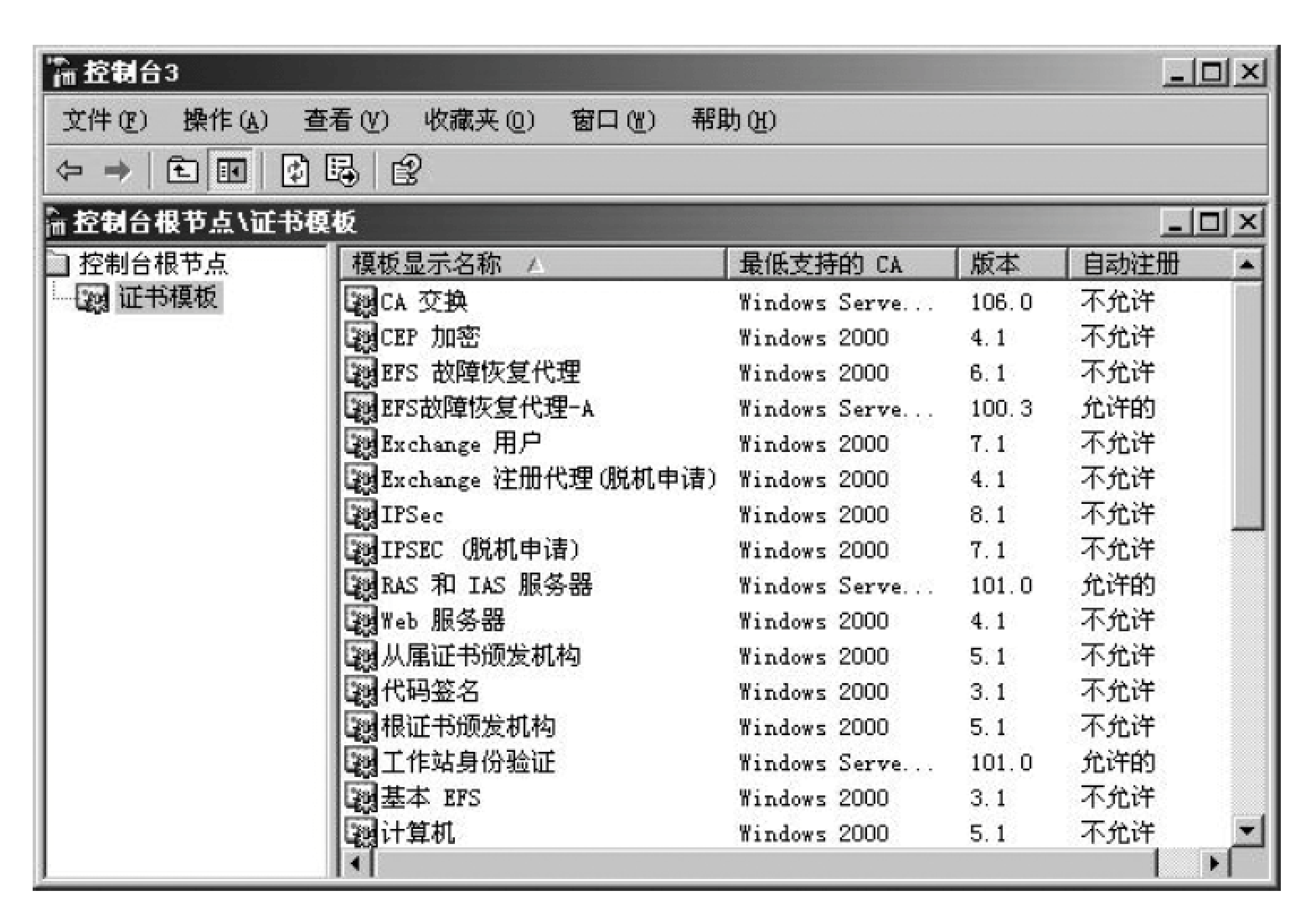


图 8-96　【证书模板】管理单元

接着要创建用户证书模板的副本。

（5）选择控制台树中的【证书模板】选项，在右侧详细信息列表窗格中的【用户】模板上右击，在弹出的快捷菜单中选择【复制模板】命令，打开如图 8-97 所示的【新模板的属性】对话框的【常规】选项卡。在其中的【模板显示名称】中输入“存档用户”。

（6）切换到如图 8-98 所示的【处理请求】选项卡，选中【把使用者的加密私钥存档】复选框。该选项可以让密钥恢复代理从证书存储区中恢复私钥。

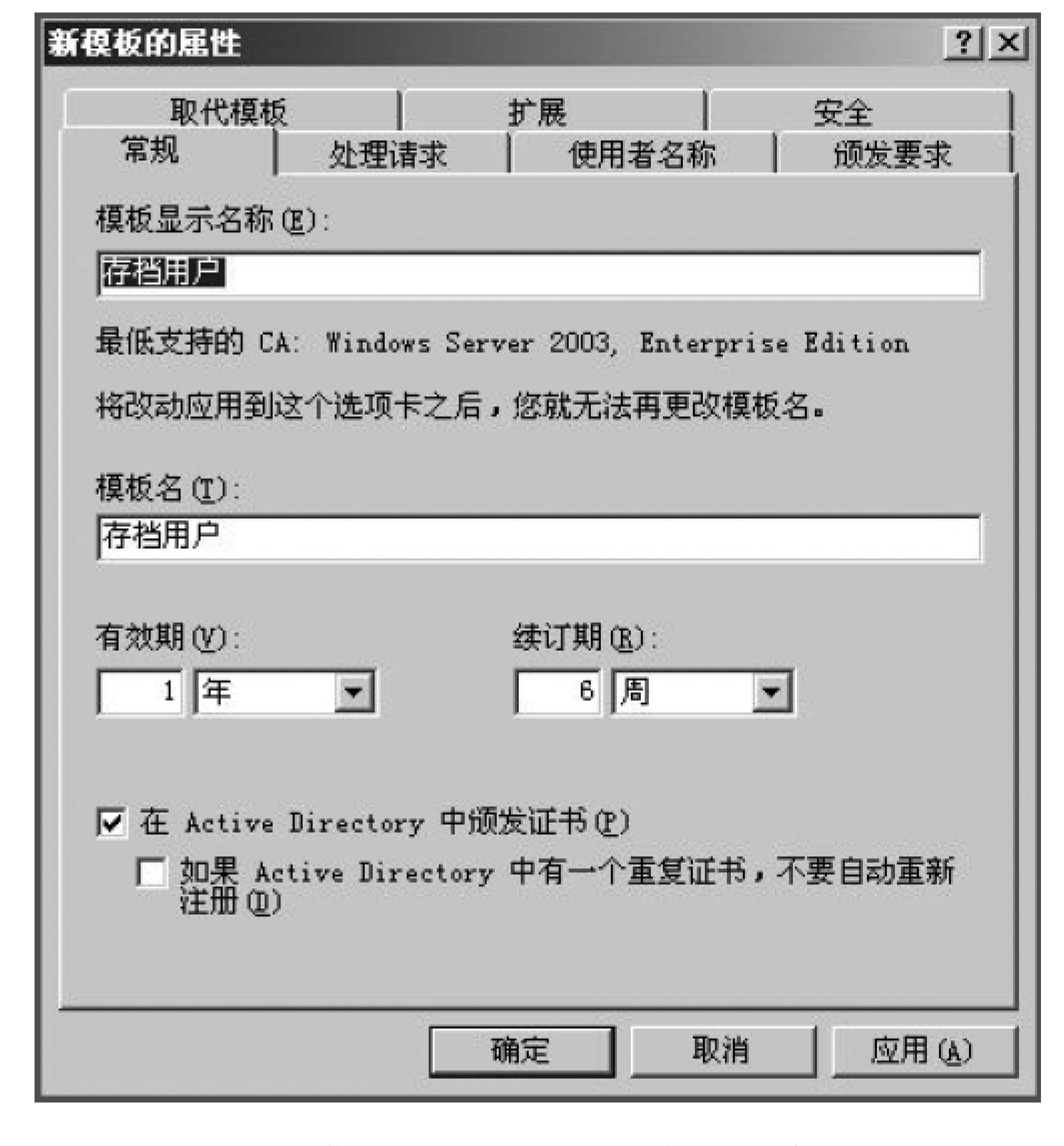


图 8-97　【新模板的属性】对话框的【常规】选项卡

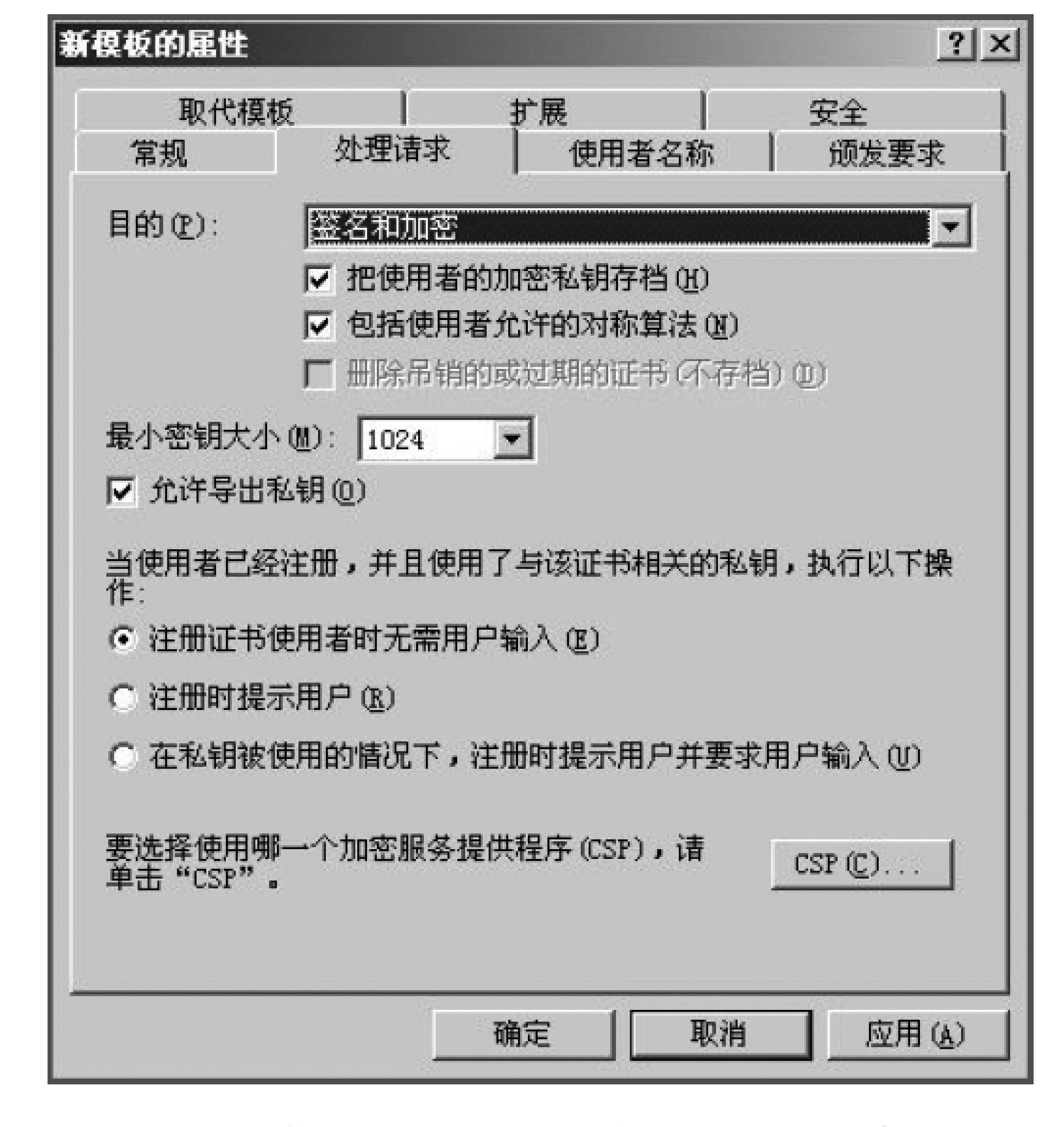


图 8-98　【新模板的属性】对话框的【处理要求】选项卡



(7) 切换到【安全】选项卡。在其中确保 Domain Admins 和 Domain Users 组成员可以注册此证书。这些权限是从【用户】证书模板中复制的。

(8) 单击【确定】按钮,可保存"控制台 3"。

5. 获取具有存档密钥的用户证书

即配置企业 CA 以颁发"存档用户"证书。

具体操作步骤如下:

(1) 以 Administrator 账户登录域控制器。配置企业 CA 以颁发新的"存档用户"证书模板。打开【证书颁发机构】控制台窗口,如图 8-87 所示。

(2) 在控制台树中的【证书模板】选项上右击,在弹出的快捷菜单中选择【新建】命令,打开如图 8-99 所示的【启用证书模板】对话框。在其中选择要颁发的证书模板—存档用户。

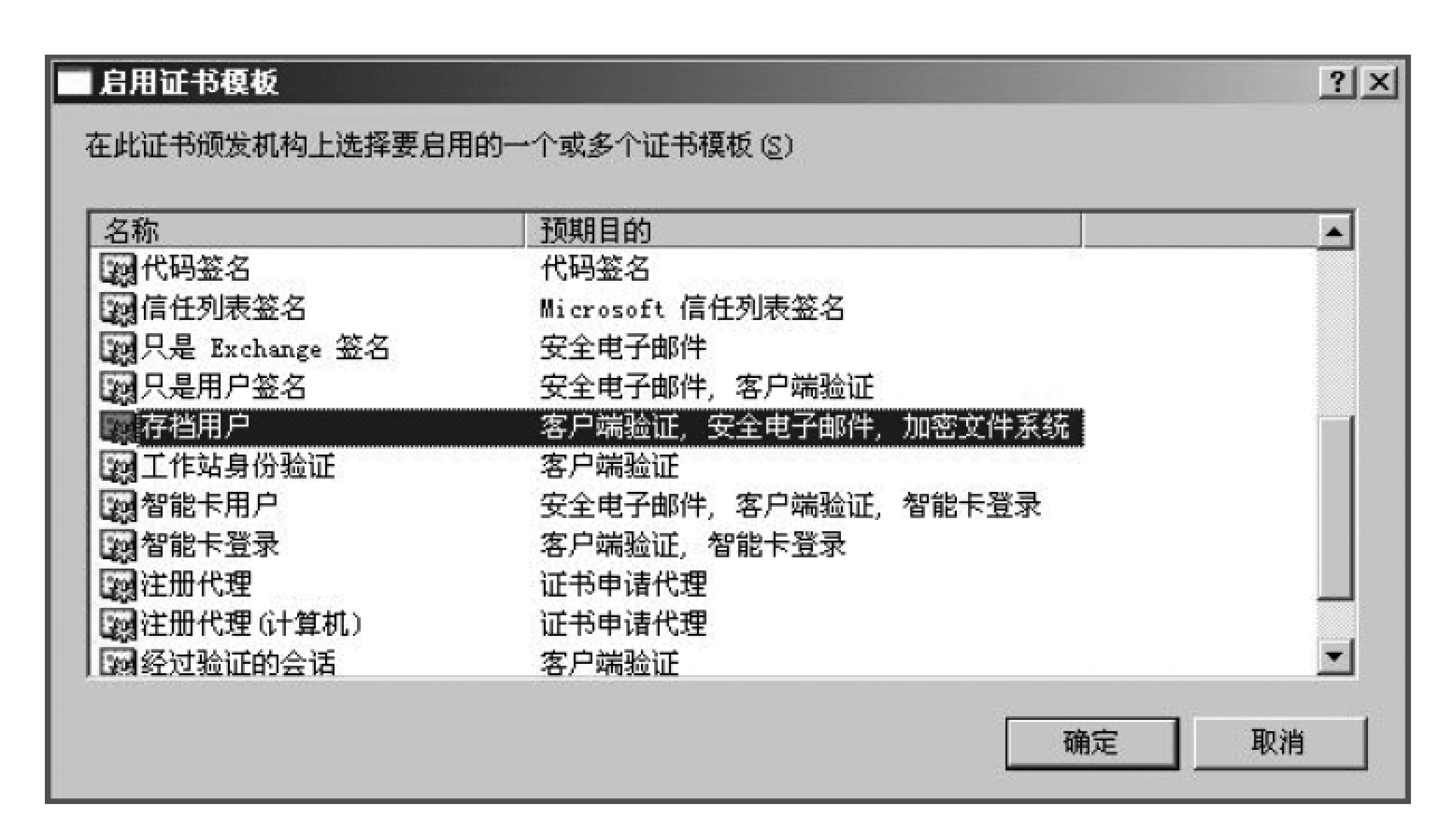


图 8-99 【启用证书模板】对话框

(3) 单击【确定】按钮,【存档用户】证书模板即出现在【证书颁发机构】的右侧详细信息列表窗格中,如图 8-100 所示。



图 8-100 "存档用户"证书模板

(4) 在【Active Directory 用户和计算机】管理单元中将原有用户 Anne 配置为隶属于



Server Operators(服务器操作员组)。并配置用户的电子邮件,如图 8-101 所示。

注意:一定要配置好用户的电子邮件,否则在下面的存档用户证书无法申请成功。另外,把用户添加到 Server Operators 组的目的是为了便于从本机登录到域控制器,因为 Server Operators 组用户默认具有登录到域控制器的权限。

(5) 以 Anne 账户登录域控制器,然后用前面介绍的方法,利用 MMC 控制台,以其账户添加个人证书管理单元。并申请一个以"存档用户"为模板的用户证书。在申请证书过程中,证书模板类型要选择前面新创建的并在 CA 中发布的"存档用户"证书模板,如图 8-102 所示。证书名称取为"存档用户",如图 8-103 所示。

(6) "存档用户"证书申请的配置摘要如图 8-104 所示。单击【完成】按钮,即可完成 Anne 用户的存档用户证书申请。此时在个人证书控制台的【个人】/【证书】选项的详细信息列表窗格中可以看到新申请的"存档用户"证书,如图 8-105 所示。



图 8-101　配置用户的电子邮件

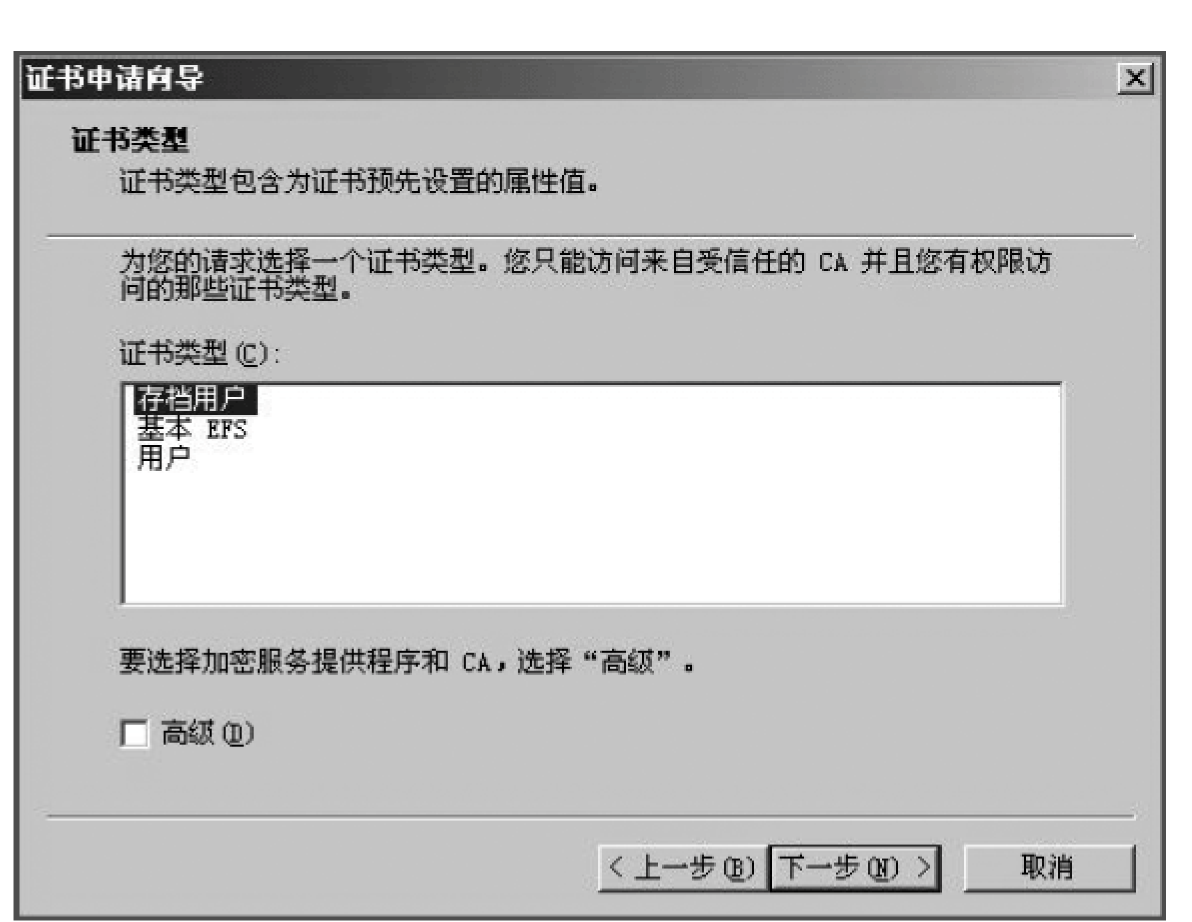


图 8-102　选择"存档用户"的【证书类型】对话框

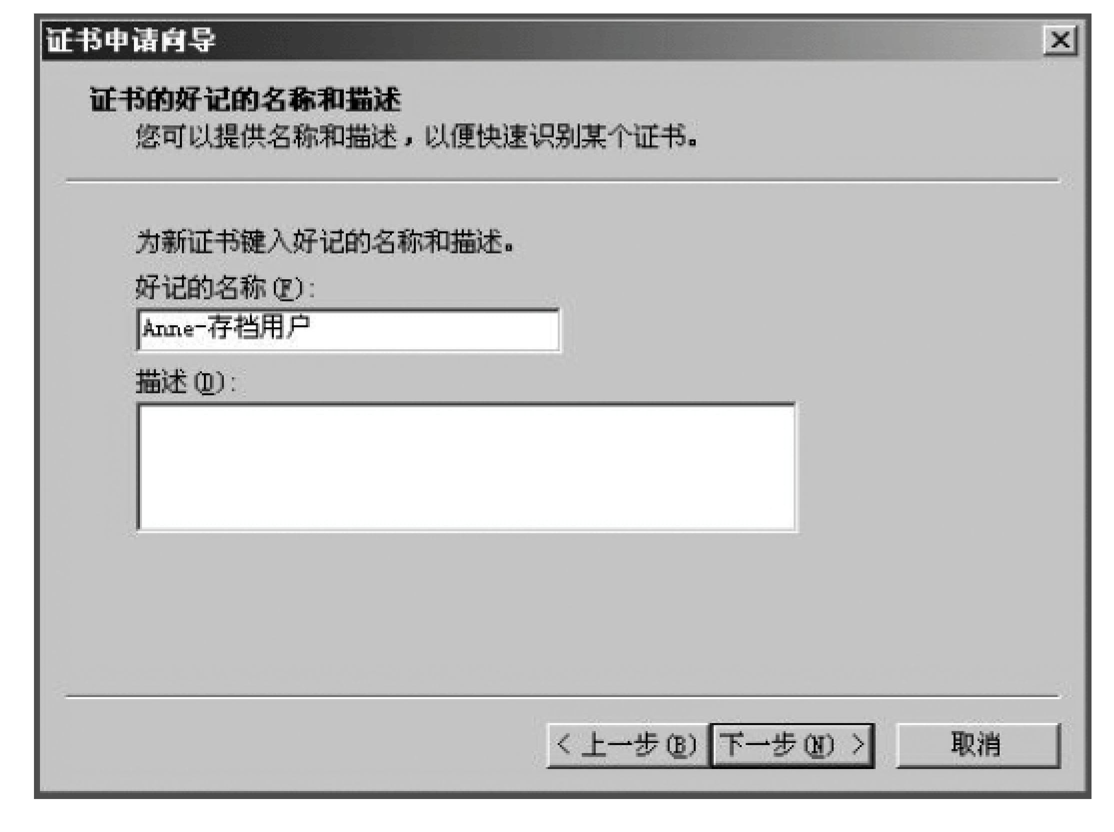


图 8-103　【证书的好记的名称和描述】对话框



图 8-104　【正在完成证书申请向导】对话框





图 8-105　在【证书】控制台中显示的新“存档用户”证书

将控制台另存为“控制台 Anne”，关闭控制台及所有窗口，并从域控制器中注销登录。

6. 执行密钥恢复

利用上一步骤创建的 Anne 用户存档证书进行密钥恢复。

具体操作步骤如下：

(1) 以 Administrator 账户登录域控制器，查看【证书颁发机构】控制台中的【存档密钥】，确保私钥可以恢复。

① 选择【开始】/【管理工具】/【证书颁发机构】命令，打开【证书颁发机构】控制台窗口，参见图 8-87。

② 在控制台树中选择【颁发的证书】选项，选择【查看】/【添加/删除列】命令，打开如图 8-106所示的【添加/删除列】对话框。



图 8-106　【添加/删除列】对话框

③ 在【添加/删除列】对话框的【可用列】列表框中选择【存档的密钥】选项，然后单击【添加】按钮，把【存档的密钥】添加到【显示列】列表中。

④ 单击【确定】按钮，返回到【证书颁发机构】对话框，选中【颁发的证书】选项，在详细信息窗格中将水平滚动条向右拖动，以确认颁发给 Anne 的证书的【存档的密钥】列中的值为“是”，如图 8-107 所示。







图 8-107　在【证书颁发机构】对话框中显示的 Anne“存档用户”证书

⑤ 双击“存档用户”证书，在打开的【证书】对话框中选择【详细信息】选项卡，如图 8-108 所示。记下证书的序列号(不要包括两个数字之间的空格)。



图 8-108　【证书】对话框中的【详细信息】选项卡

注意：证书的序列号是长度为 20 个字符的十六进制字符串，私钥的序列号与证书的序列号相同，该序列号是进行密钥恢复所必需的。

⑥ 单击【确定】按钮返回到【证书颁发机构】对话框，关闭【证书颁发机构】控制台。

(2) 使用 Certutil.exe 将私钥恢复到私钥输出文件。

① 选择【开始】/【运行】命令，输入 cmd 并按 Enter 键，进入命令提示符状态，确保当前路径为 C:\。

② 在命令提示符下，输入如下命令：

```
C:\>Certutil-getkey[证书的序列号]AnneERP
```



其中,[证书的序列号]为上面记下的那 20 位序列号(不带空格),AnneERP 为将私钥恢复的私钥输出文件,在此取名为:AnneERP(也可以取别的文件名)。

③ 在命令提示符下输入如下命令:

```
C:\>dir AnneERP
```

即可列出 AnneERP 文件,如图 8-109 所示。如果找不到 AnneERP 文件,说明输入的[证书的序列号]可能不正确。AnneERP 文件包含 KRA(密钥恢复代理)证书、用户证书和 PKCS#7。

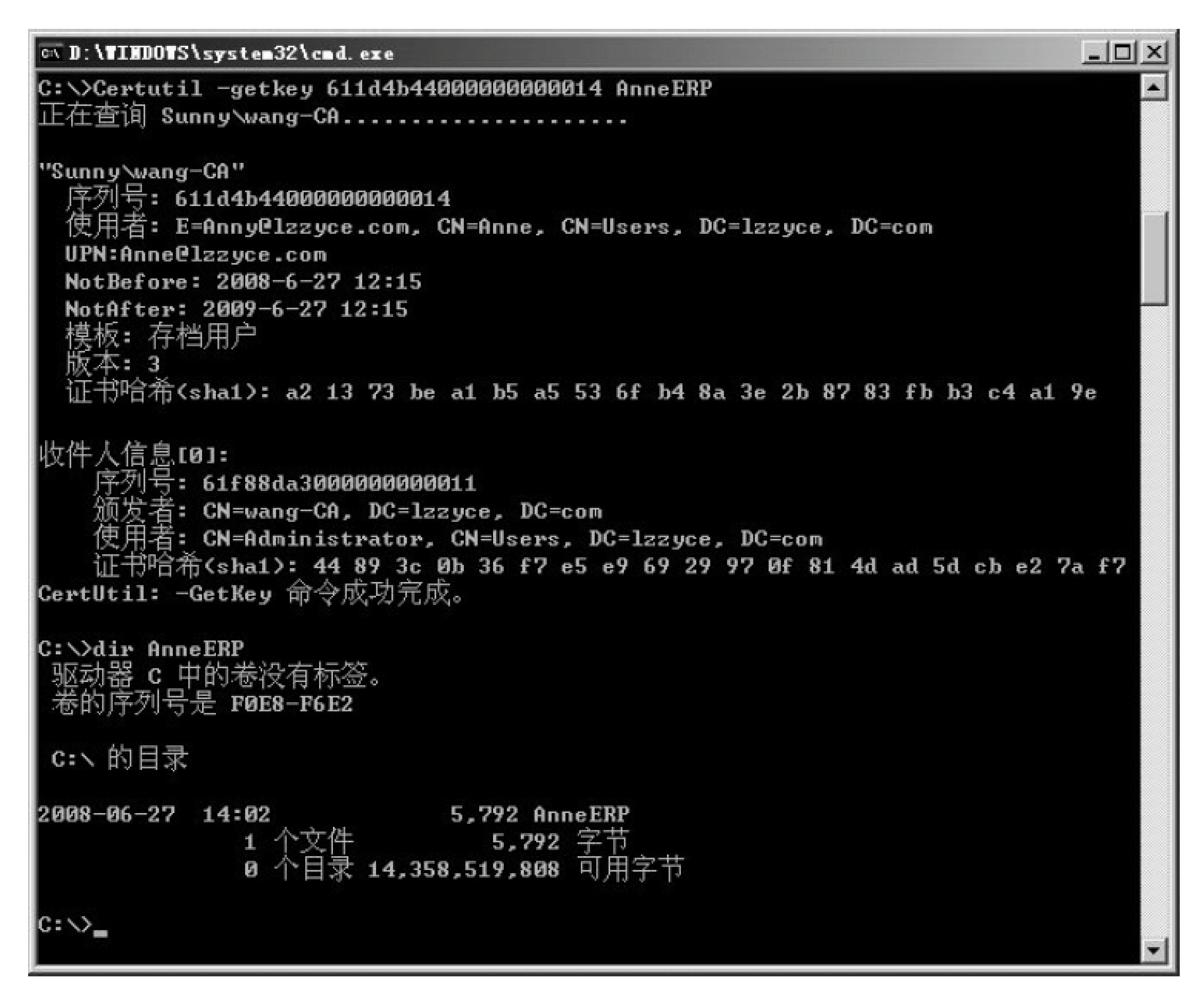


图 8-109 将私钥恢复到文件的命令过程

(3) 使用 Certutil.exe 命令恢复原始公/私钥对。

① 在命令提示符下输入如下命令:

```
C:\>Certutil-recoverkey AnneERP Anne.pfx
```

其中,Anne.pfx 为公/私钥对文件,在此取名为:Anne.pfx(也可以取别的文件名,但扩展名不能改变)。

② 当系统给出要输入密码的提示时,则输入新密码,并确认新密码。

③ 输入 exit 命令,然后按 Enter 键,关闭所有窗口并注销当前用户。

上述执行过程如图 8-110 所示。

7. 导入已恢复的私钥

通过导入 Anne.pfx 文件还原 Anne 的证书存储区中已恢复的私钥。以 Anne 账户登录域控制器。

具体操作步骤如下:

(1) 以 MMC 控制台方式添加【证书】管理单元。







图 8-110　执行 Certutil-recoverkey 命令的结果

（2）在【证书】控制台的【证书(当前用户)】控制台树上右击，在弹出的快捷菜单中选择【查找证书】命令，打开如图 8-111 所示的【查找证书】对话框。



图 8-111　【查找证书】对话框

（3）在【包含】文本框中，输入证书颁发机构名(如本实验中的 wang-CA)，单击【立即查找】按钮。然后选择如图 8-112 所示 Anne 的"存储发现在"为"个人"的证书，删除该证书，以模拟重新安装的计算机。

（4）关闭【查找证书】对话框。接下来要导入 Anne. pfx 证书。

（5）在【证书】控制台树的【个人】项上右击，在弹出的快捷菜单中选择【所有任务】/【导入】命令，打开如图 8-113 所示的【欢迎使用证书导入向导】对话框。





图 8-112　选择 Anne 的“存储发现在”为“个人”的证书

(6) 单击【下一步】按钮，打开如图 8-114 所示的【要导入的文件】对话框。在该对话框的【文件名】文本框中输入/导出的公/私钥对文件 C:\Anne.pfx。

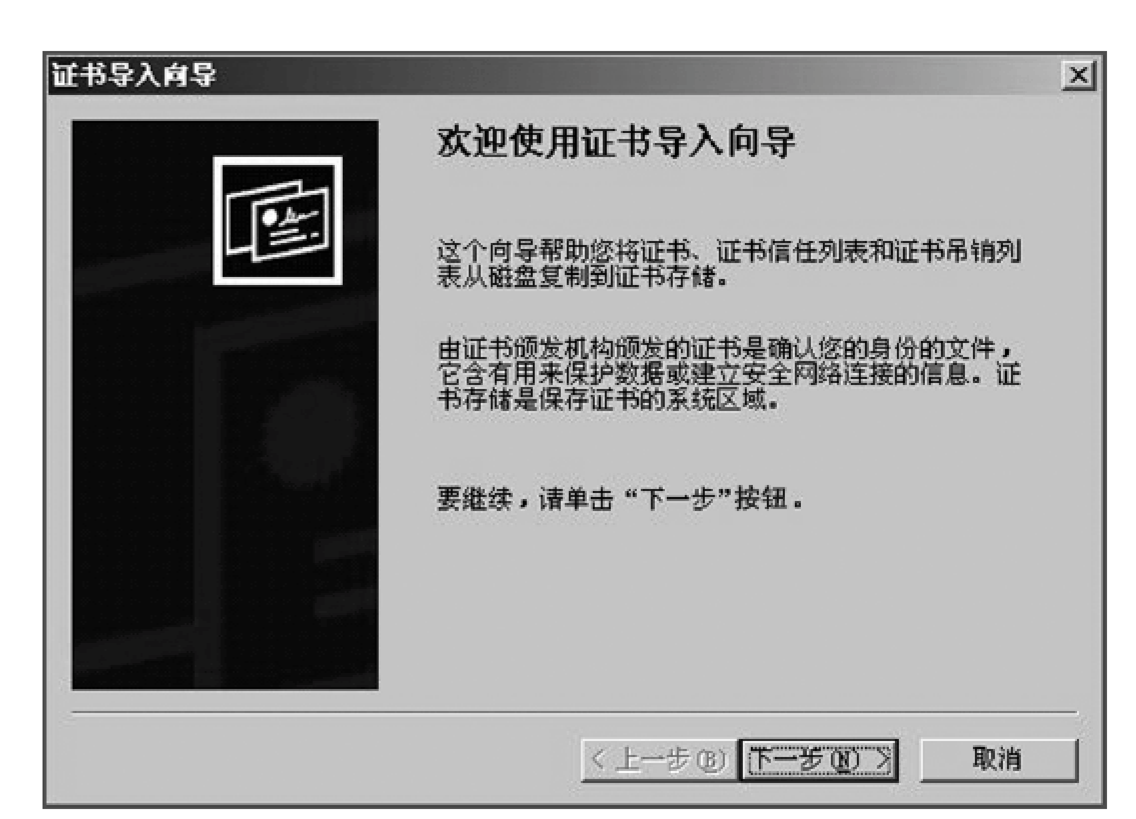


图 8-113　【欢迎使用证书导入向导】对话框

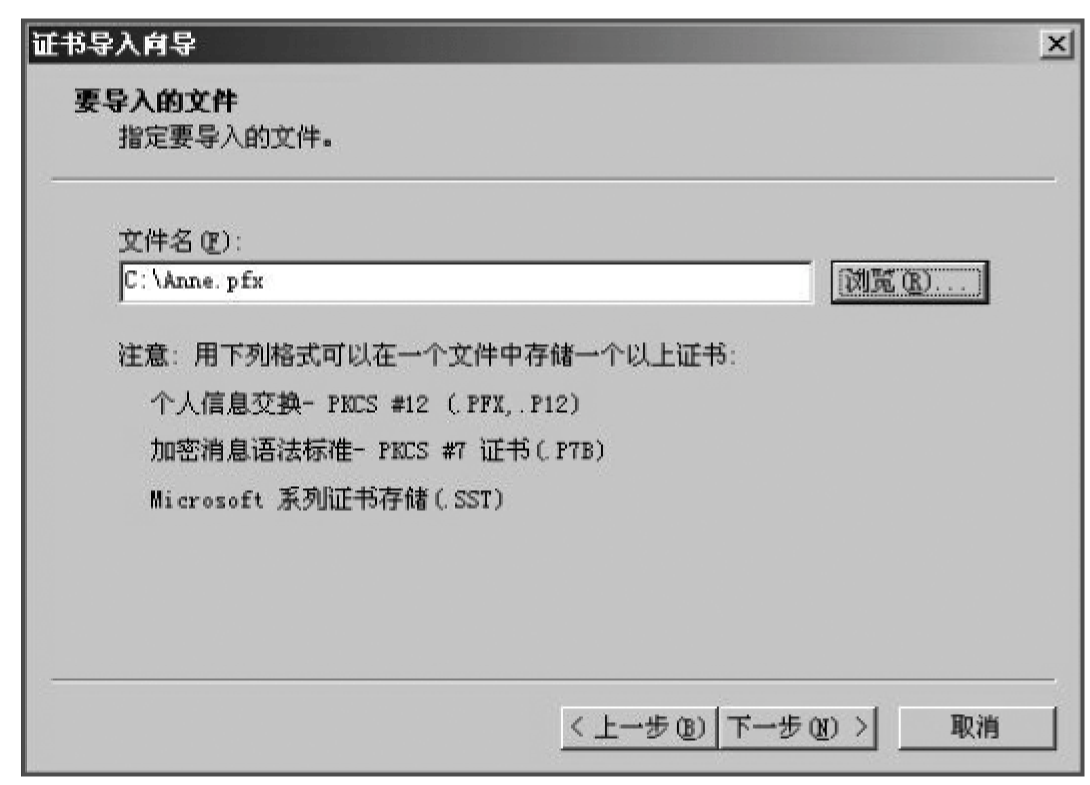


图 8-114　【要导入的文件】对话框

(7) 单击【下一步】按钮，打开如图 8-115 所示的【密码】对话框。在【密码】文本框中输入/导出公/私钥正确时配置的新密码。

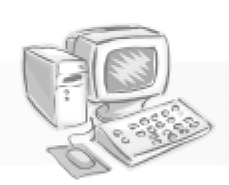
(8) 单击【下一步】按钮，打开如图 8-116 所示的【证书存储】对话框。在此对话框中选择【根据证书类型，自动选择证书存储】单选按钮。

(9) 单击【下一步】按钮，打开如图 8-117 所示【正在完成证书导入向导】对话框。单击



图 8-115　【密码】对话框





【完成】按钮，最后提示导入成功。此时 Anne 用户的两个证书都已被导入。Anne 的“存档用户”证书位于“个人”证书存储区，而证书颁发机构证书位于“受信任的根证书颁发机构”存储区。

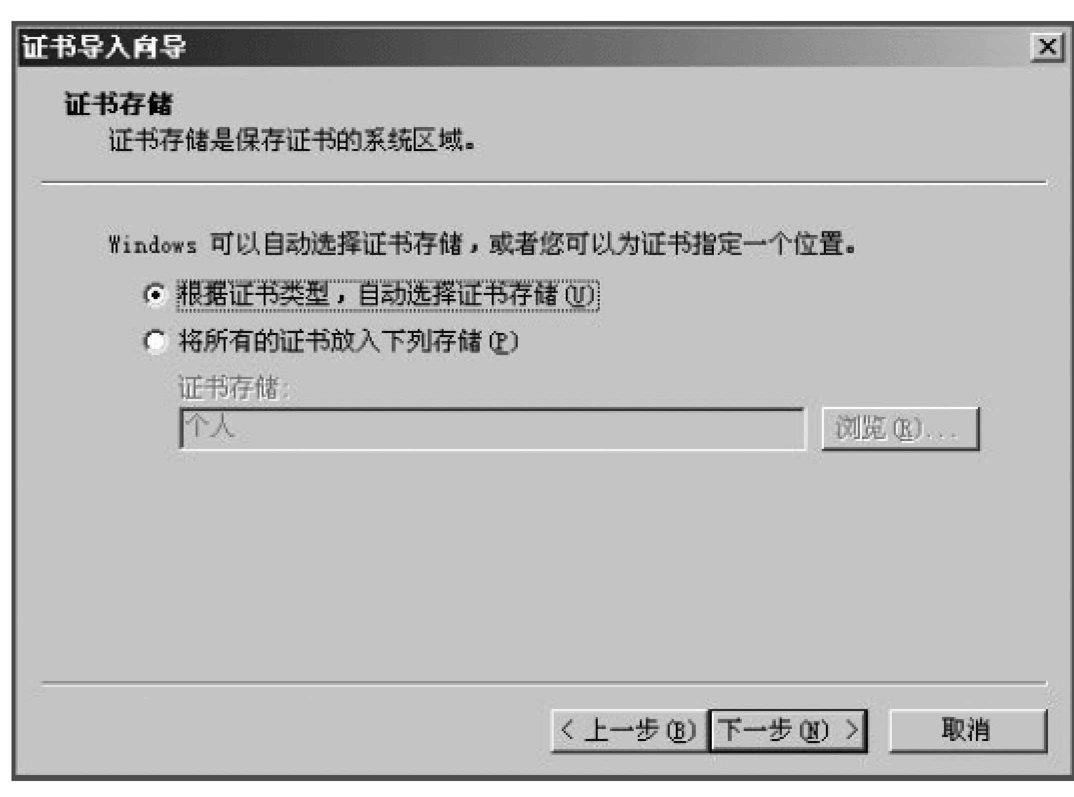



图 8-116　【证书存储】对话框



图 8-117　【正在完成证书导入向导】对话框

我们还可以验证导入的证书的序列号，选择【证书】控制台树的【个人】/【证书】命令，双击证书，在打开的对话框中选择【详细信息】选项卡，即可验证序列号是否与原来的序列号相匹配。

(10) 关闭所有打开的窗口，并注销用户账户。至此，已完成整个密钥恢复代理的创建和在密钥丢失后恢复密钥的全过程。

8.6　邮件的加密和数字签名

8.6.1　邮件安全技术

由于越来越多的人通过电子邮件发送机密信息，因此确保电子邮件安全变得日趋重要。数字证书最常见的应用就是发送安全邮件，即利用安全邮件证书对电子邮件签名和加密，既保证了发送的邮件不是伪造的，又保证了第三者无法阅读加密邮件的内容。

邮件加密技术采用多种加密方法，可以通过 RSA 公钥体系为例简述其原理。RSA 加密基于一个无法对大素数进行分解质因子的数学假设，使用两个大素数的函数，一个作为公共密钥；另一个作为私人密钥，由于这两个密钥是互补的，公共密钥加密的密文可以用私人密钥解密；反之亦然。因此，邮件发送者只需要使用收件人的公共密钥加密邮件，加密后的邮件只有拥有私人密钥的收件人才能解密阅读，从而确保了邮件的安全。

当用户使用自己的电子证书在发出的邮件上签名时，邮件将被按照邮件的内容通过摘要函数运算取得一个可以用以检验邮件完整性的值，并将该值使用电子证书中的私人密钥加密，然后与公共密钥和邮件内容一起发送出去。由于私人密钥加密的内容只有对应的公共密钥可以解密，并且摘要函数可以在任意大小的数据中采集一个固定长度的摘要，供采集的数据源即使有一位数据改变取得的结果也不同，邮件的内容有任何改变都无法与原来检验邮件完整性的值相匹配，当收件人收到邮件时，即可知道邮件的内容是否被篡改，同时也知道该邮件发送者使用的是哪一个电子证书。由于第三方的权威证书颁发机构 CA 在发出



电子证书时，将验证申请者是否拥有所申请电子邮箱的使用权，收件人也就能够通过证书发行机构验证发件人所使用的电子证书，确认所收到的邮件的确来自拥有这个邮箱地址的用户，从而实现对发件人的真实性与邮件内容是否完整的鉴别。

邮件安全技术非常复杂，但使用起来非常方便，不论是签名还是加密、解密，具体的步骤都将由电子邮件客户端软件实施。目前 FoxMail、Outlook Express 与 Outlook 等主流的电子邮件客户端软件都能够支持。用户需要做的只是申请电子证书，并在电子邮件客户端软件上指定每个电子邮件地址将使用哪种电子证书。在需要为发送的电子邮件签名或加密时单击相应的按钮即可完成。接收经过签名或加密的邮件时，验证邮件是否完整和解密的工作将由电子邮件客户端软件自动完成。

现在全球三大数字证书颁发机构 Verisign、Thawte 和 Geotrust，其中 Thawte 和 Geotrust 已经被 Verisign 收购，成为其全资子公司。Thawte 是一个专门为邮件系统颁发免费数字证书的公司，下面我们以申请该公司的数字证书为例，介绍安全发送邮件的方法。

8.6.2 邮件的加密和数字签名步骤

发送数字签名和加密的邮件需要经过如图 8-118 所示操作步骤。

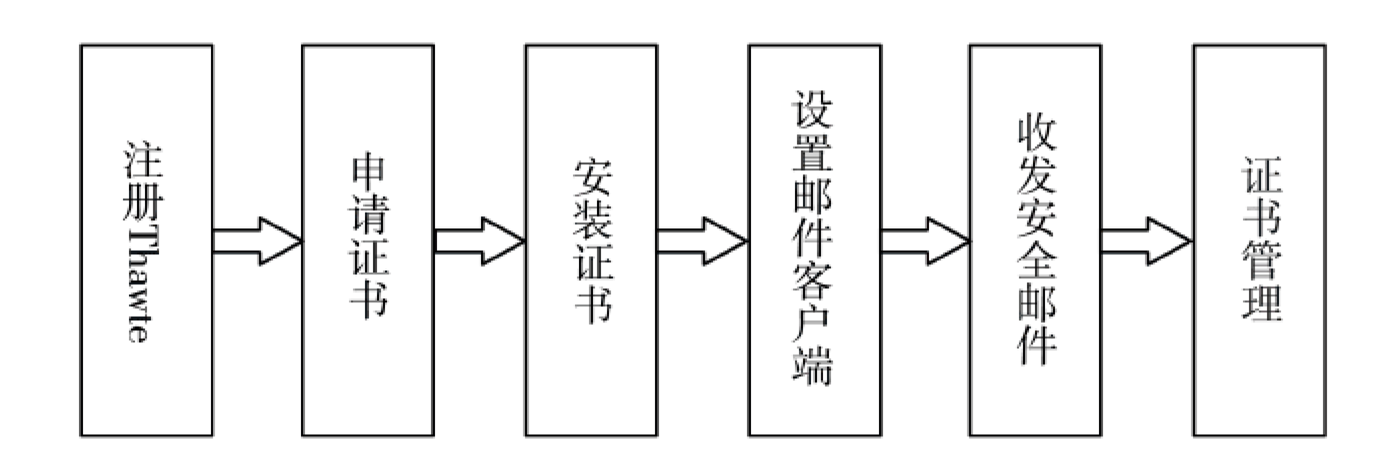


图 8-118　邮件加密和数字签名的操作步骤

1. 注册 Thawte

(1) 登录 http://www.thawte.com，选择中间导航栏上的 Products/ Free Personal E-mail certificates(生成/免费的个人邮件证书)命令，如图 8-119 所示，打开个人邮件证书页面(图 8-120)，单击页面上方的 Join 按钮，即可进行注册。

> **注意：** Thawte 上几乎所有的 Web 程序都采用.exe 扩展名，因此如果你的系统上安装了 FlashGet 之类根据文件扩展名自动下载的工具软件，需要暂时设置下载软件不监视浏览器上的单击动作。

(2) Thawte 提供一个向导式的注册页面，单击 next 按键，在 Charset For Text Input (设置输入文字类型)下拉菜单中选择你将以哪种语言输入个人信息，建议以英文输入个人信息(姓名、出生日期、国籍)，避免在未来证书处理时出现错误，如图 8-121 所示。单击 next 按键，在打开的 Requesting ID Information 页面中填写你的邮箱地址，如图 8-122 所示。

(3) 单击 next 按键，在打开的对话框中使用默认的设置 Use mybrowser settings 即可。单击 next 按键，打开如图 8-123 所示页面，进行密码设置。单击 next 按钮，打开如图 8-124 所示页面，在此设置不少于 5 个问答以用于忘记密码时验证身份。



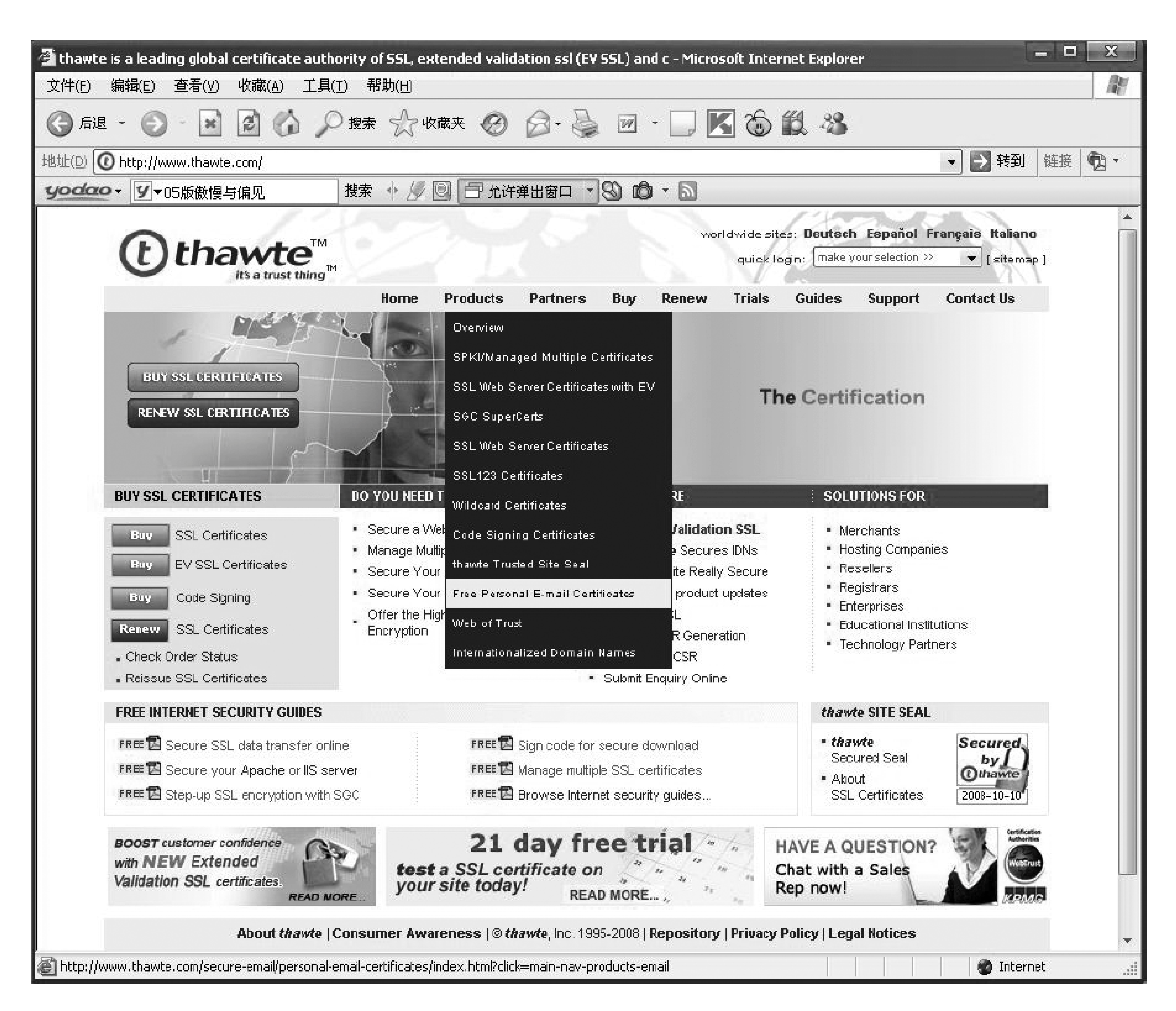


图 8-119　Thawte 主界面

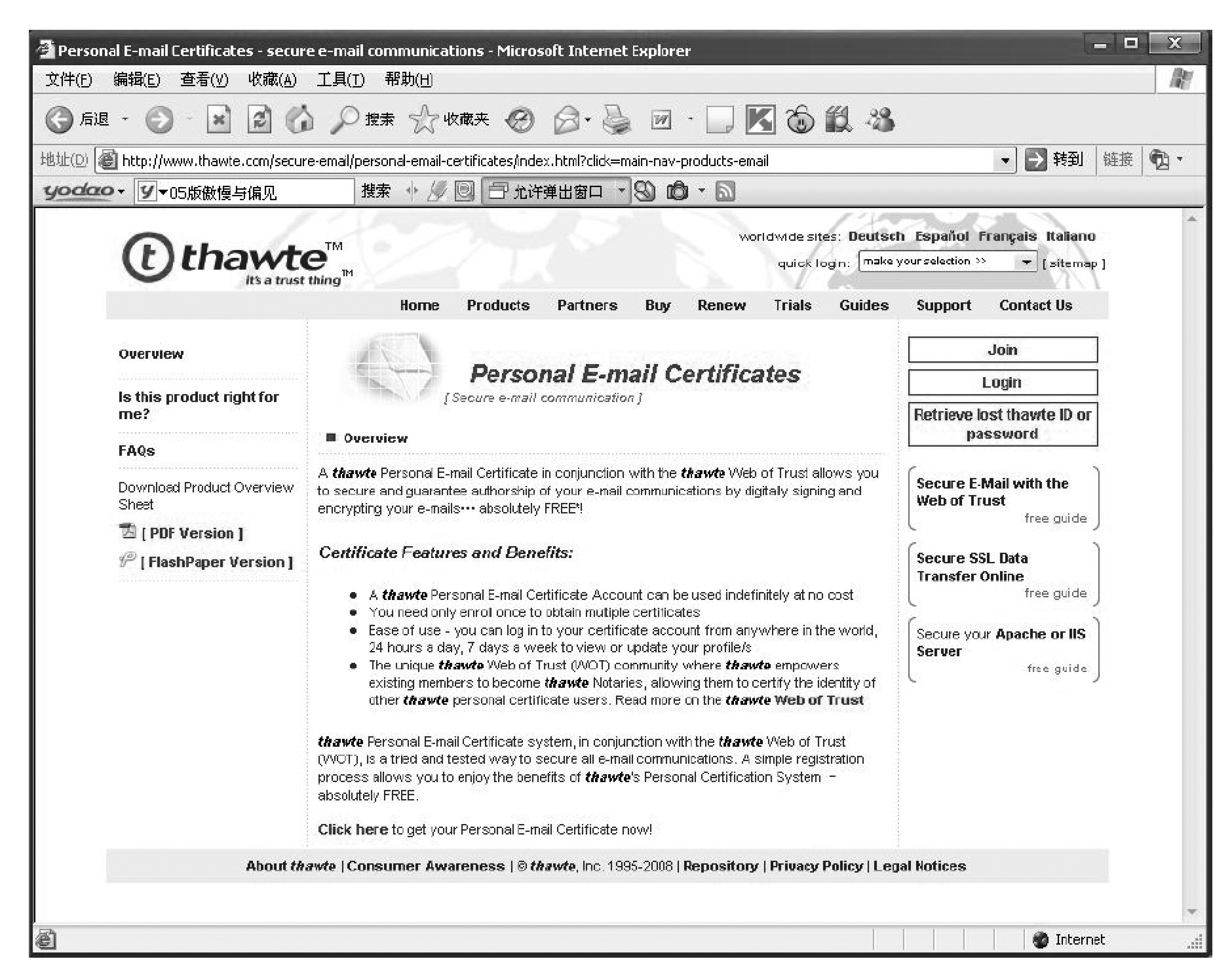


图 8-120　个人邮件证书页面



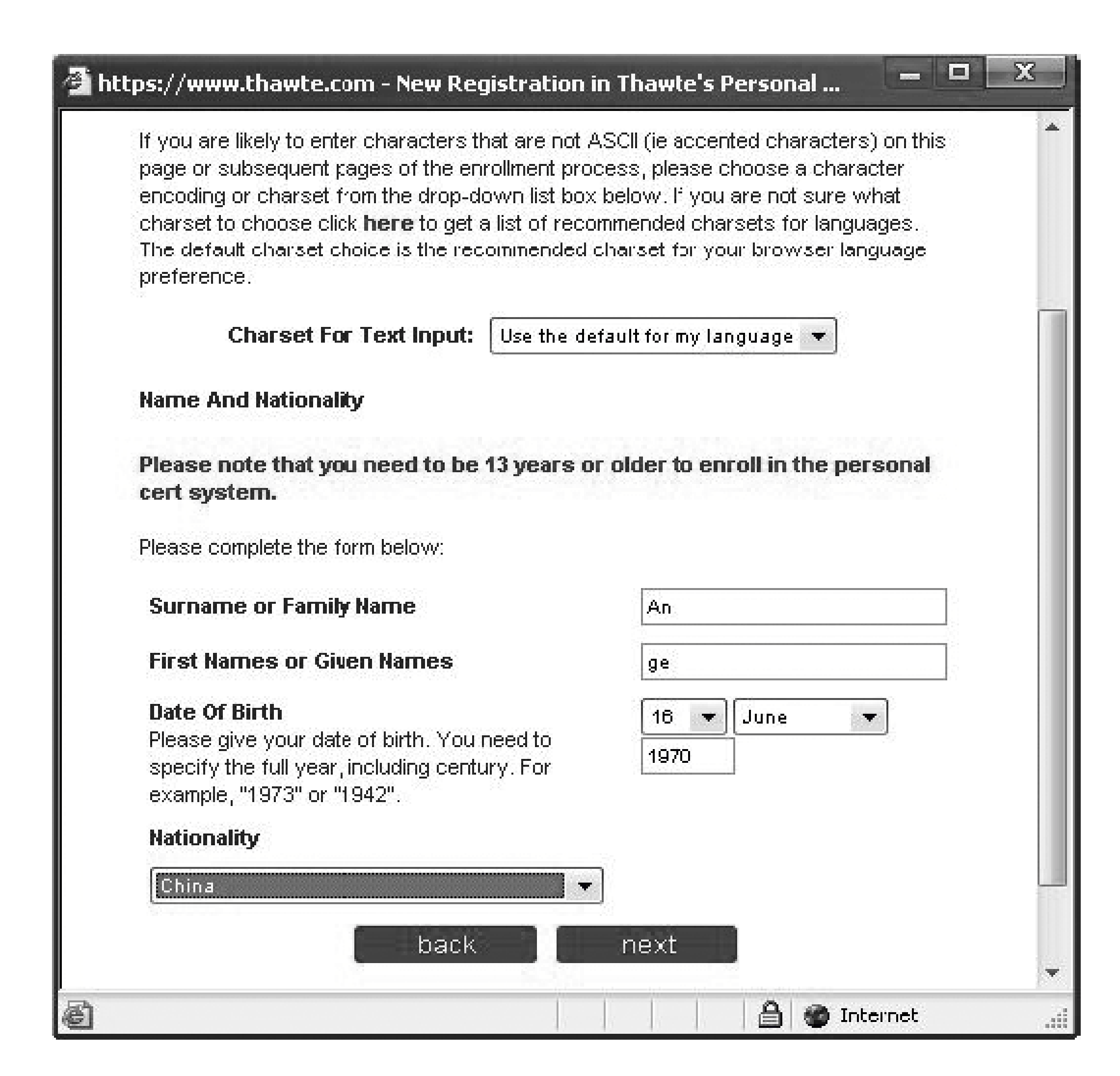


图 8-121　填写个人信息页面

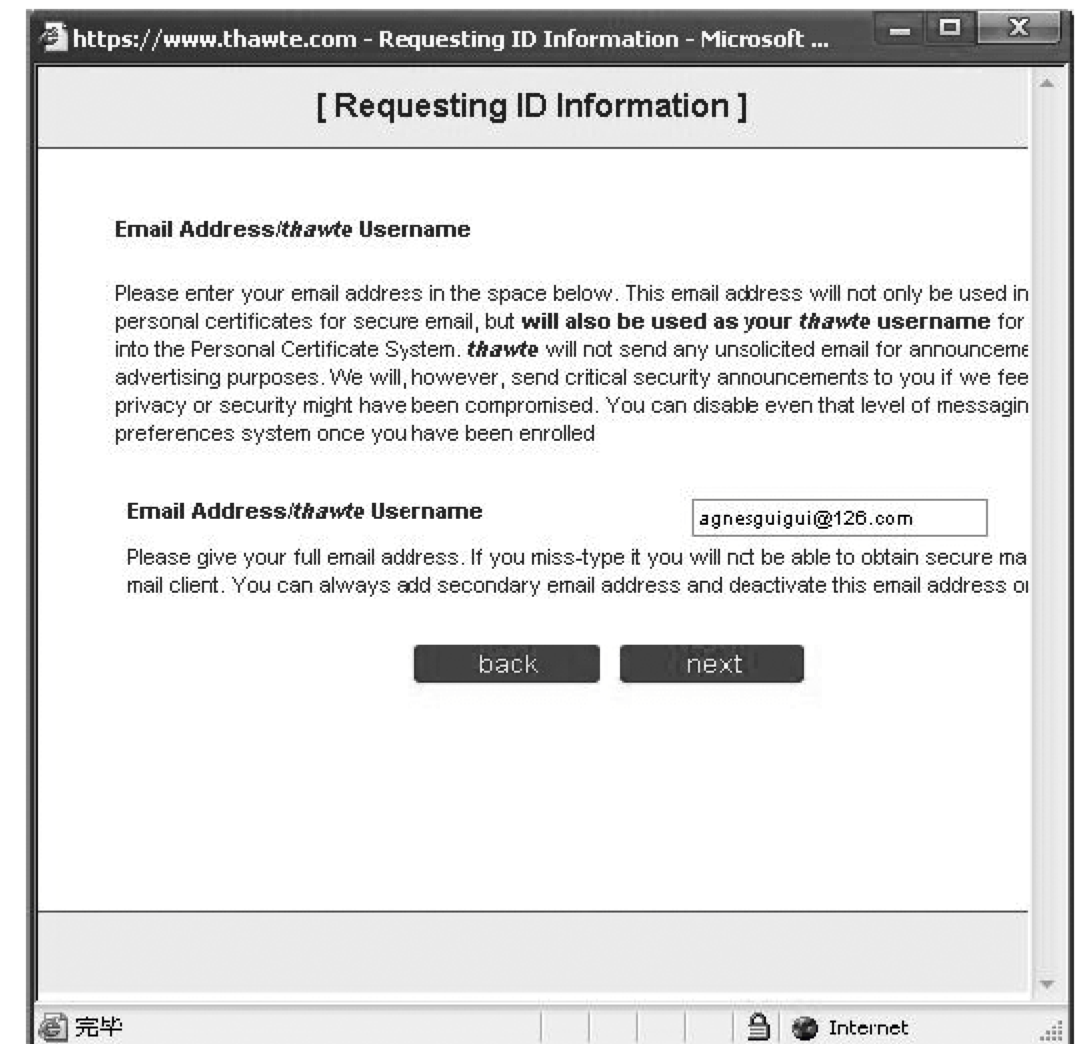


图 8-122　Requesting ID Information 页面

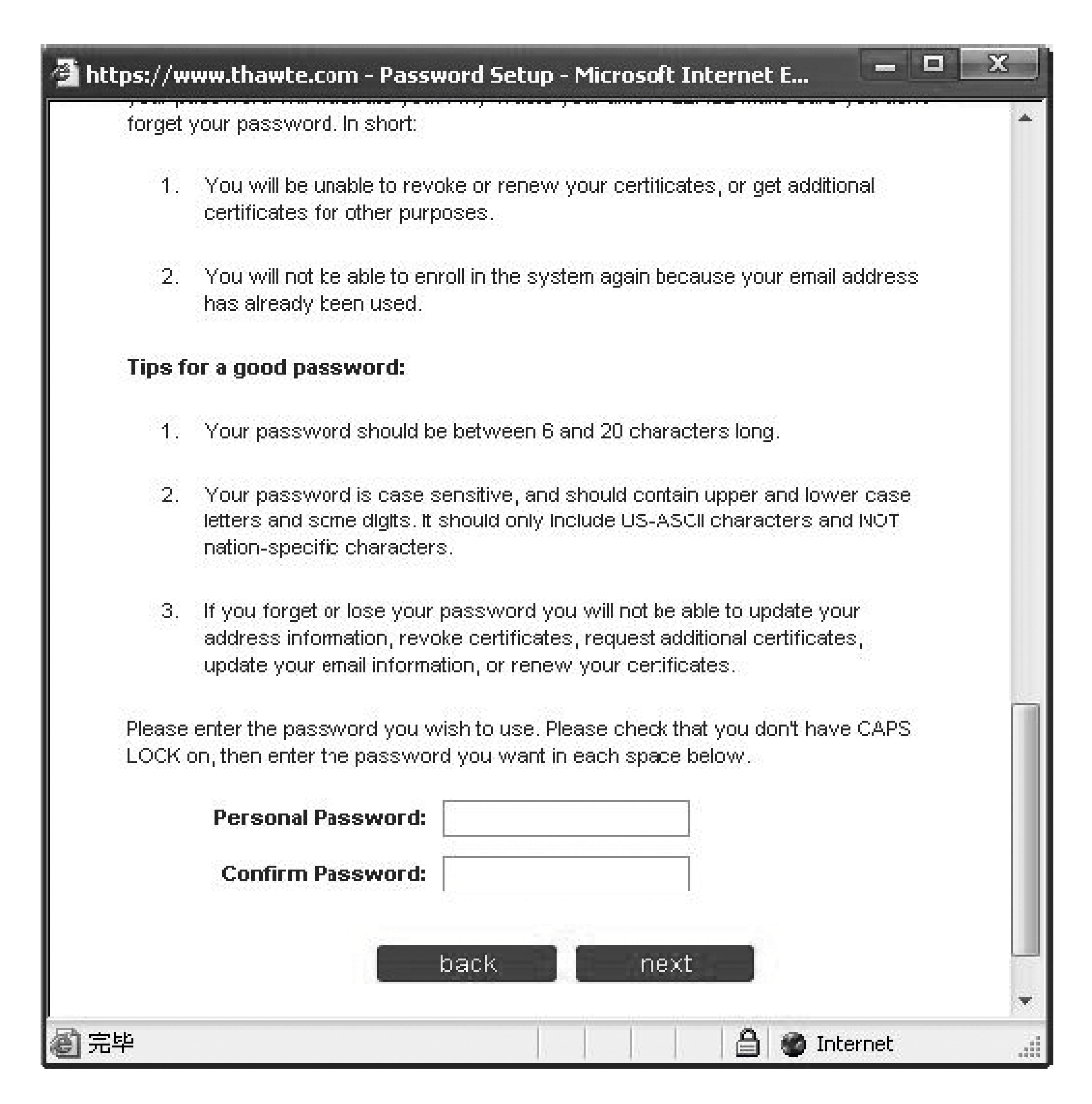


图 8-123　进行密码设置页面

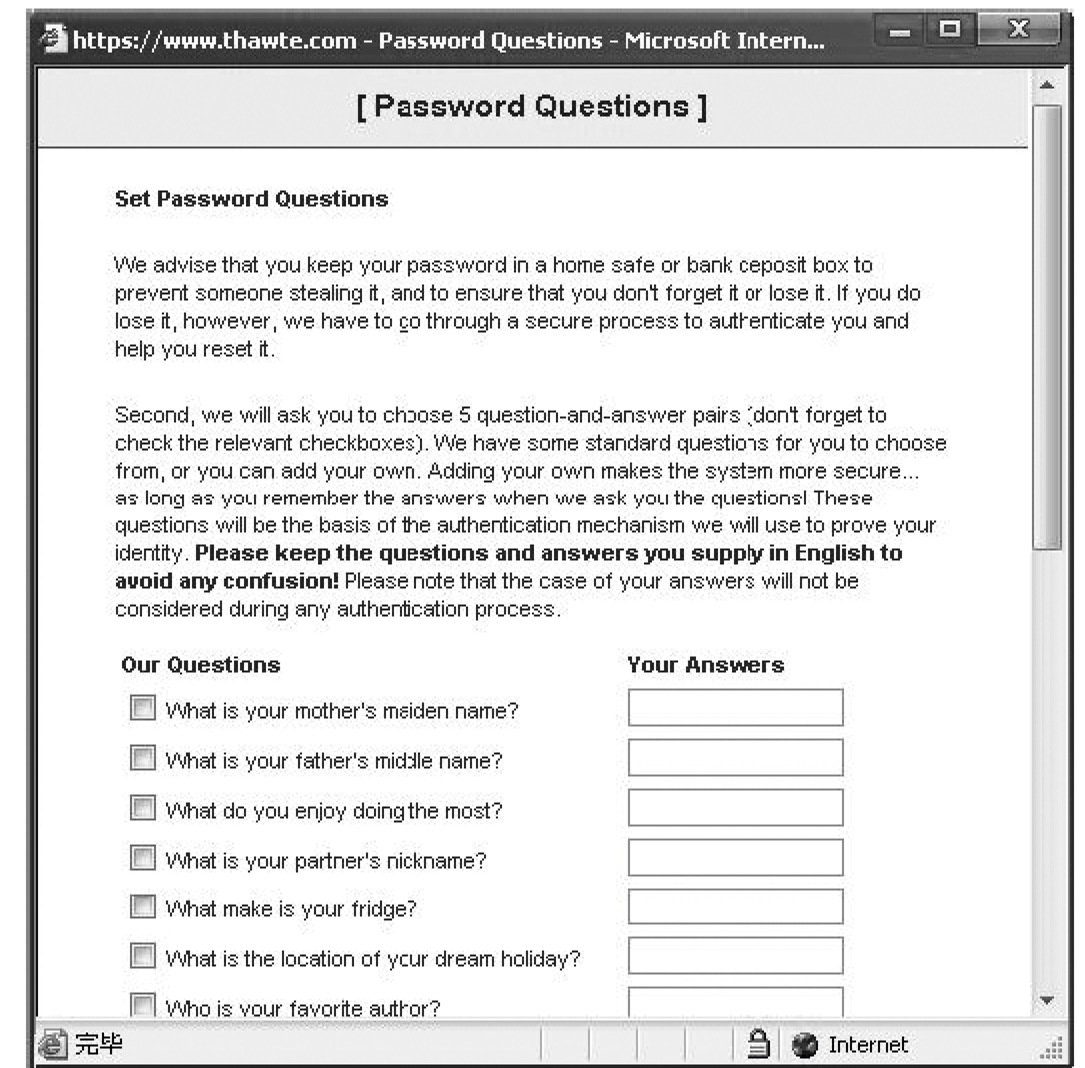


图 8-124　设置问题与答案页面

注意：你可以在网站设定的问题中选择回答也可以自己设定问题，但注意总数不少于 5 个；否则无法进入下一步。

(4) 单击 next 按钮，打开如图 8-125 所示 Please Confirm Enrollment Information(请确定注册信息)页面，如果确定注册的信息无误，单击 next 按钮，打开 Mail Ping Sent(邮件发送)页面，如图 8-126 所示，告知你需要接收网站的验证邮件并按邮件中的提示进行操作，证明你的确拥有该电子邮箱的使用权。



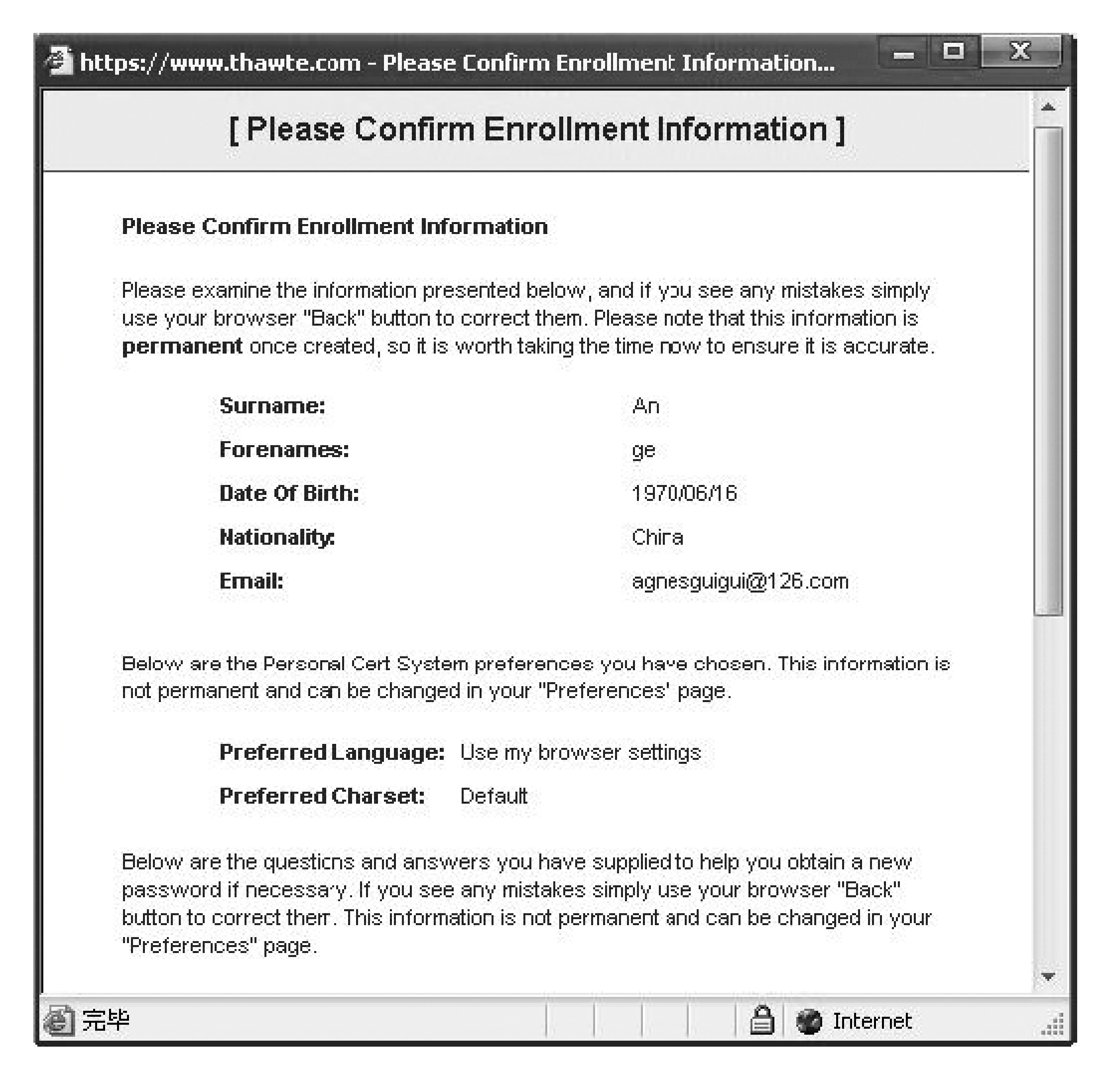


图 8-125　Please Confirm Enrollment Information 页面



图 8-126　Mail Ping Sent 页面

(5) 打开你的邮箱中来自 Thawte 的验证邮件，使用浏览器打开邮件中指定的链接 https://www.thawte.com/cgi/enroll/personal/step8.exe，如图 8-127 所示，并在页面上 Probe 和 Ping 右边的两个文本框中输入邮件中对应的内容。单击 next 按钮，打开完成注册页面，如图 8-128 所示。

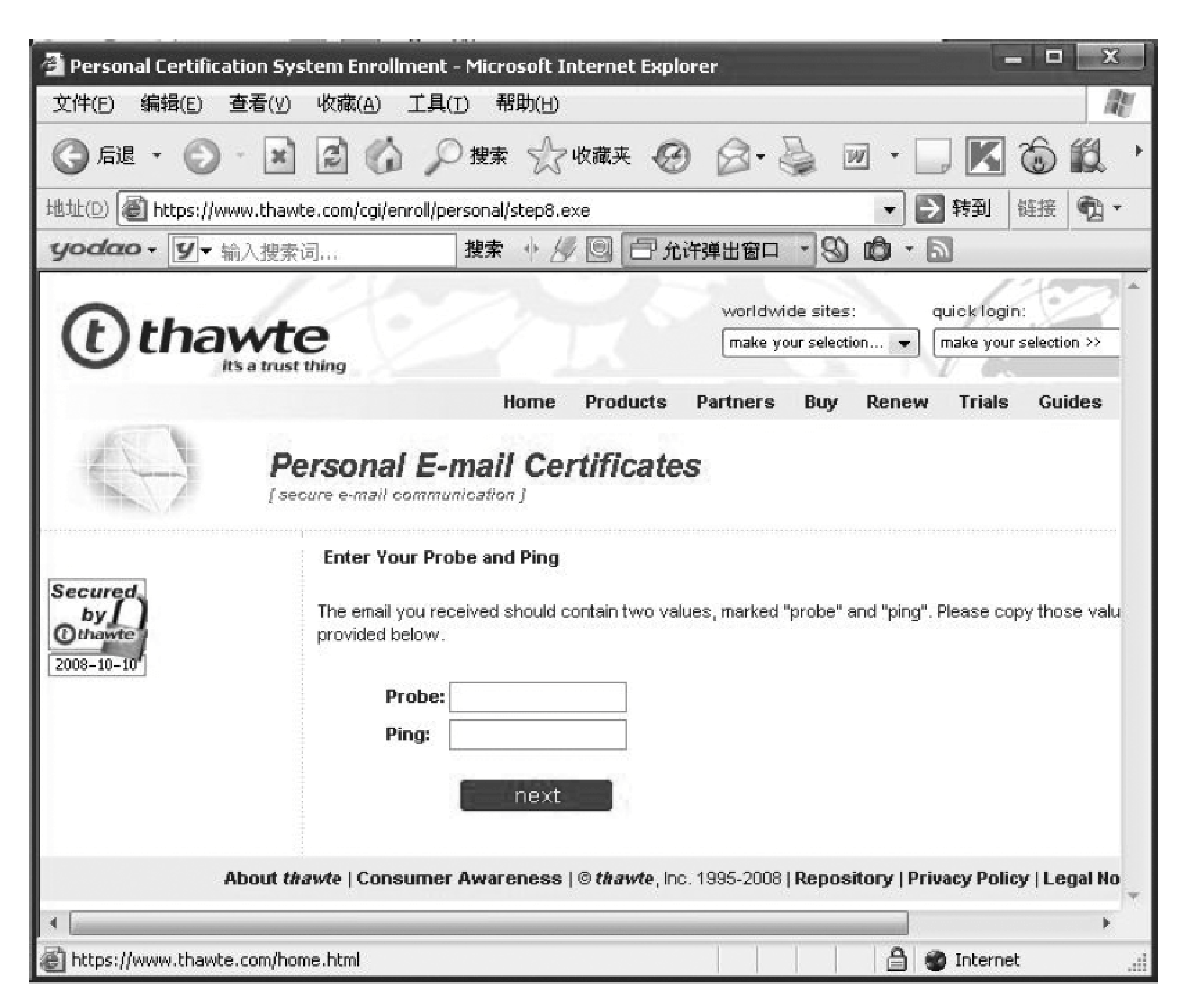


图 8-127　邮箱中指定的链接页面



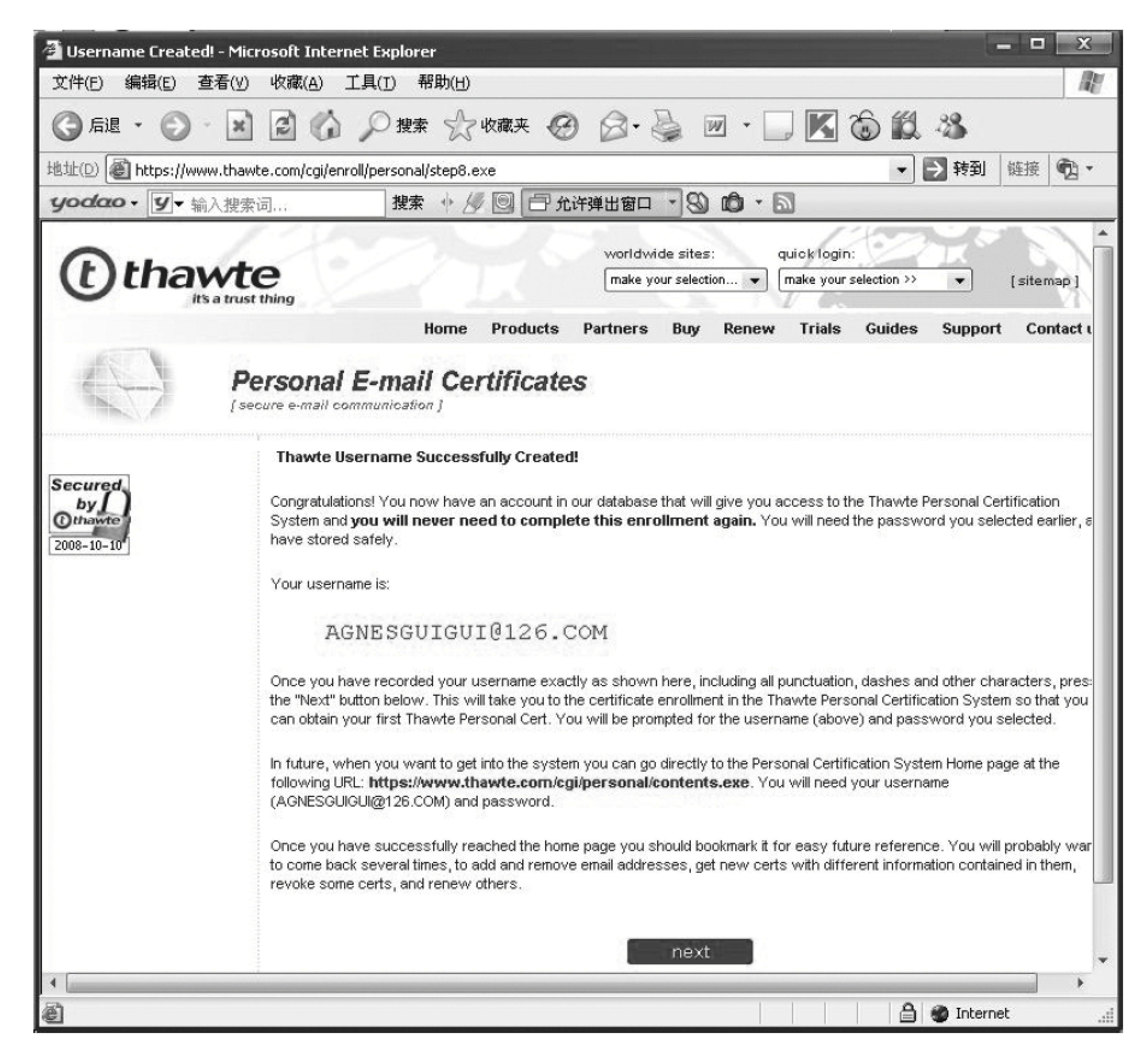


图 8-128　完成注册页面

2. 申请证书

(1) 在图 8-128 页面上单击 next 按钮(或者回到网站的首页再次进入个人邮件证书页面单击 login 按钮),在弹出的【登录】窗口(图 8-129)中使用刚才注册的账户登录。

(2) 初次登录网站将自动定位到证书申请页面(图 8-130),单击 request 按钮,打开数字证书申请向导,申请向导的步骤很多,只需一直单击 next 按钮采用默认选项即可。唯一需要注意的是,当步骤进行到 configure X.509v3 certificate extensions(配置证书范围)时(图 8-131),页面上有两个按钮,此时可以单击 accept(接受)按钮选择默认配置。



图 8-129　【登录】窗口

注意:在申请证书的过程中,网站会要求我们自己选择要包括在其中的电子邮件地址。由于你是第一次申请,网站默认只为你注册时填写的电子邮件地址生成证书,但实际上你可以将多个电子邮件地址包括在一个电子证书中。



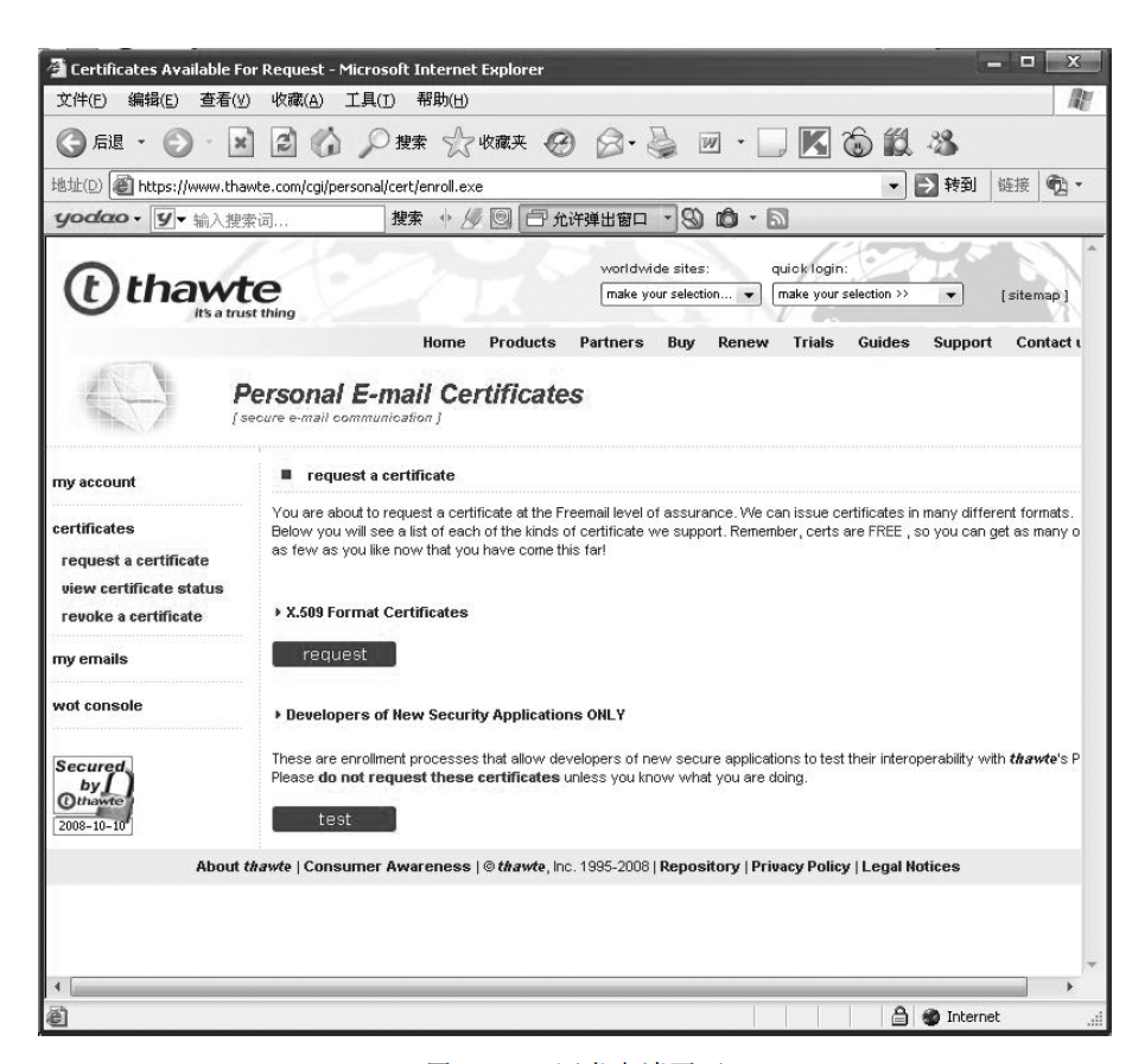


图 8-130　证书申请页面

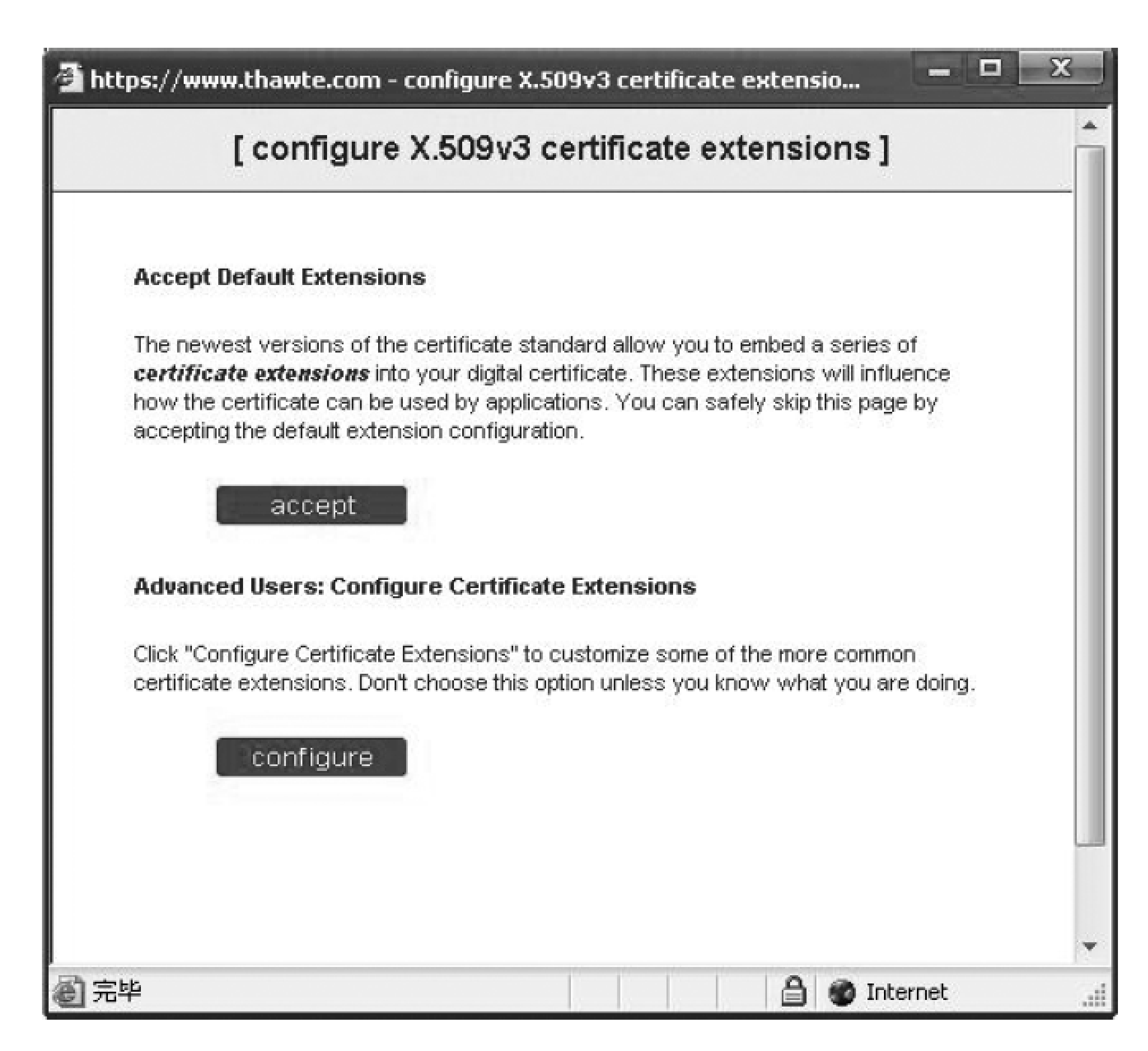


图 8-131　configure X. 509v3 certificate extensions 页面



3. 安装证书

操作步骤如下：

(1) 回到刚才登录时的操作界面(图 8-130)，选择 certificates / view certificate status(证书/查看证书状态)选项，主窗口显示如图 8-132 所示。单击 Status 栏显示为 pending(未安装)的证书 MSIE。



图 8-132　certificates / view certificate status 页面

(2) 打开证书详细信息页面如图 8-133 所示，在该页面下方单击 Fetch(取得)按钮，打开 Install Your MSIE Certificate(安装你的 MSIE 证书)页面，如图 8-134 所示。

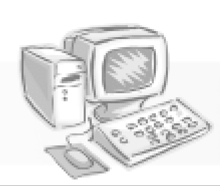
(3) 单击 Install Your Cer(安装你的证书)按钮，把刚才申请的证书安装到你的系统上。在安装证书的过程中系统将两次弹出对话框，要求确认在当前系统上安装证书。安装成功即出现如图 8-135 所示确认框，单击【确认】按钮完成安装。

4. 设置邮件客户端

获得电子证书后，需要在自己使用的电子邮件客户端软件设置相关的选项，然后才可以使用数字证书签名或加密邮件，下面介绍在 FoxMail 上的设置和使用方法。

(1) 在 FoxMail 中选择相应账户，右击，在弹出的快捷菜单中选择【属性】命令，打开【邮箱账户设置】对话框，在左侧窗口中选择【安全】选项，如图 8-136 所示。





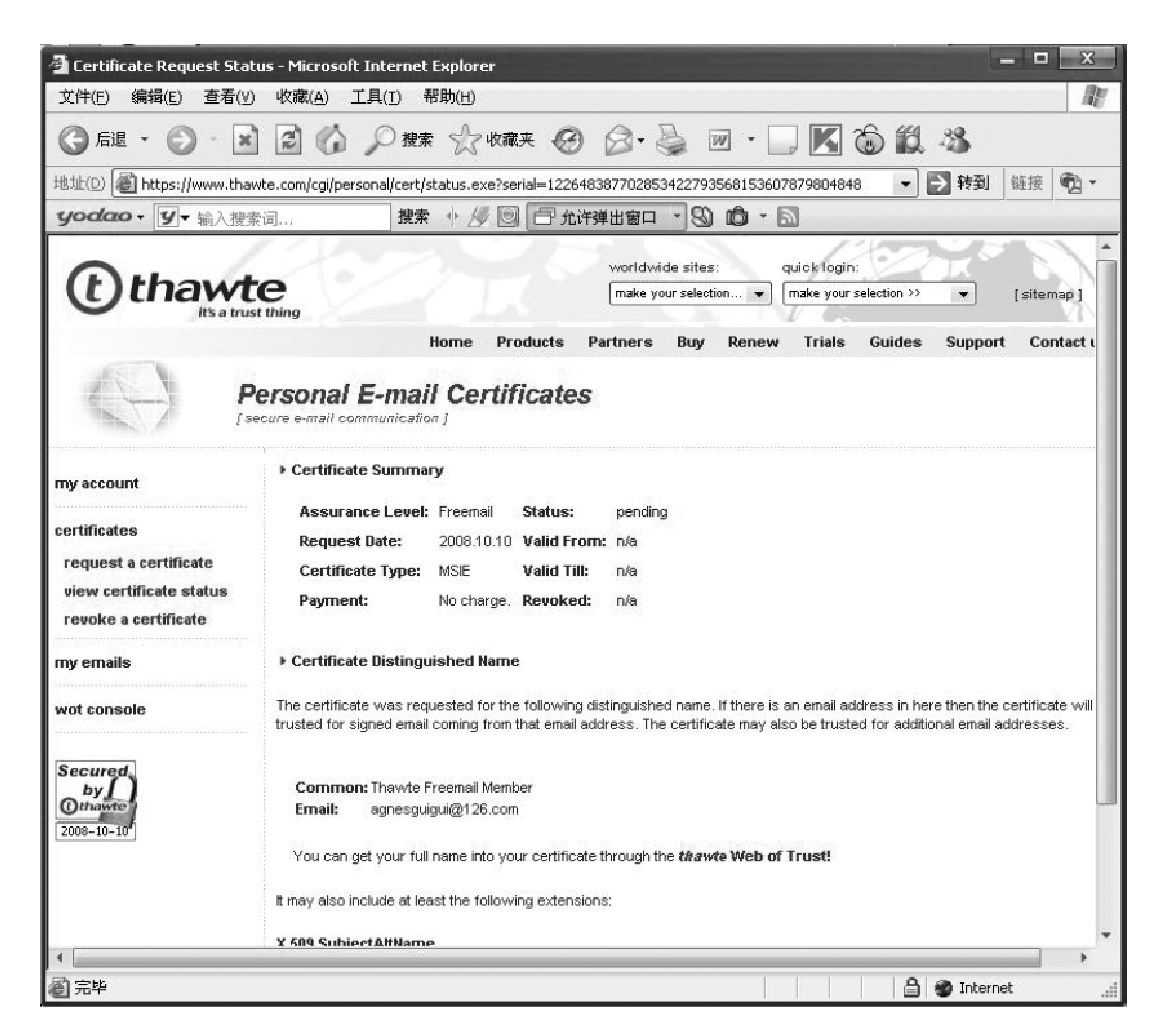


图 8-133 证书详细信息页面

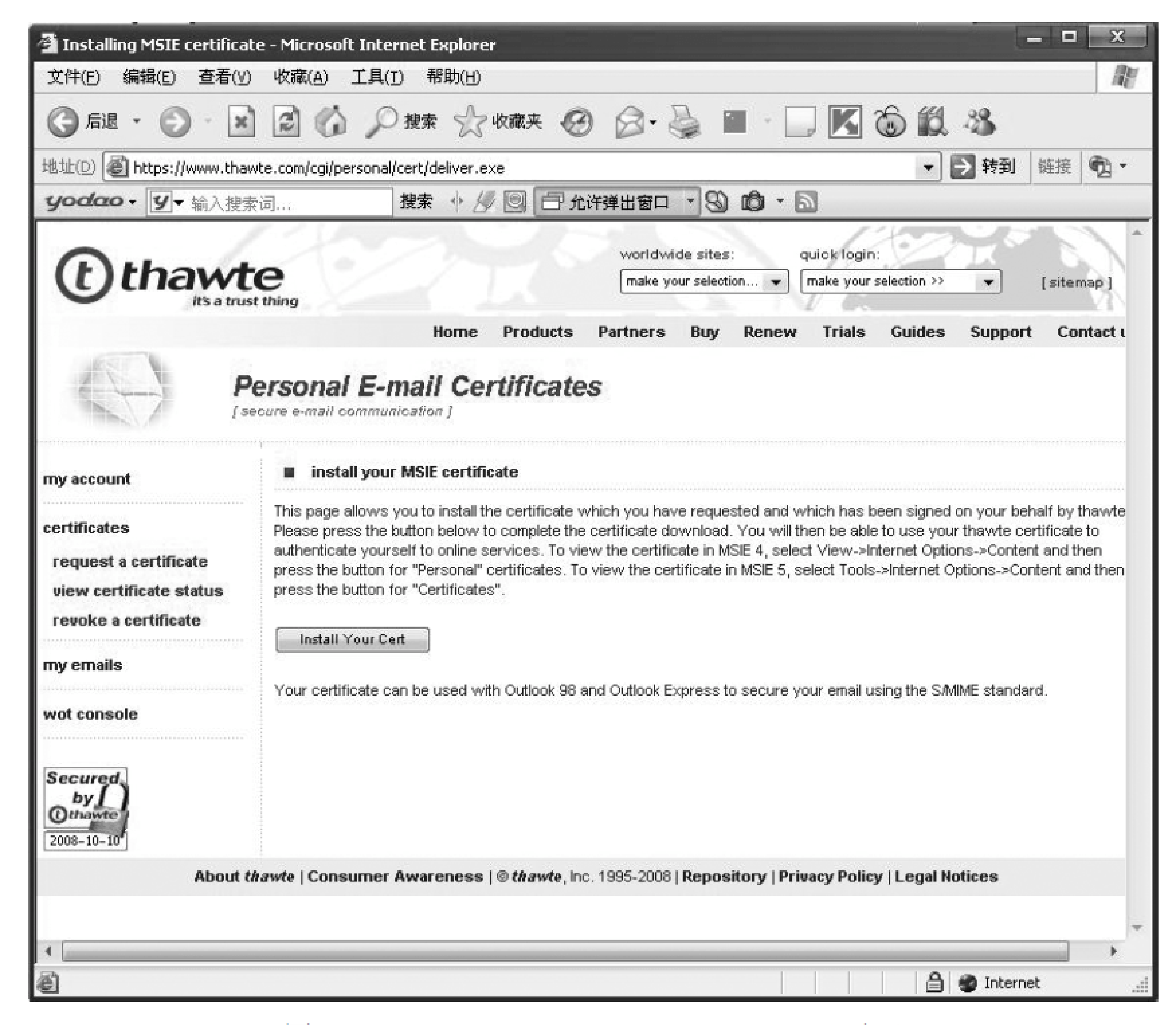


图 8-134 Install Your MSIE Certificate 页面





图 8-135 【证书安装成功】确认框

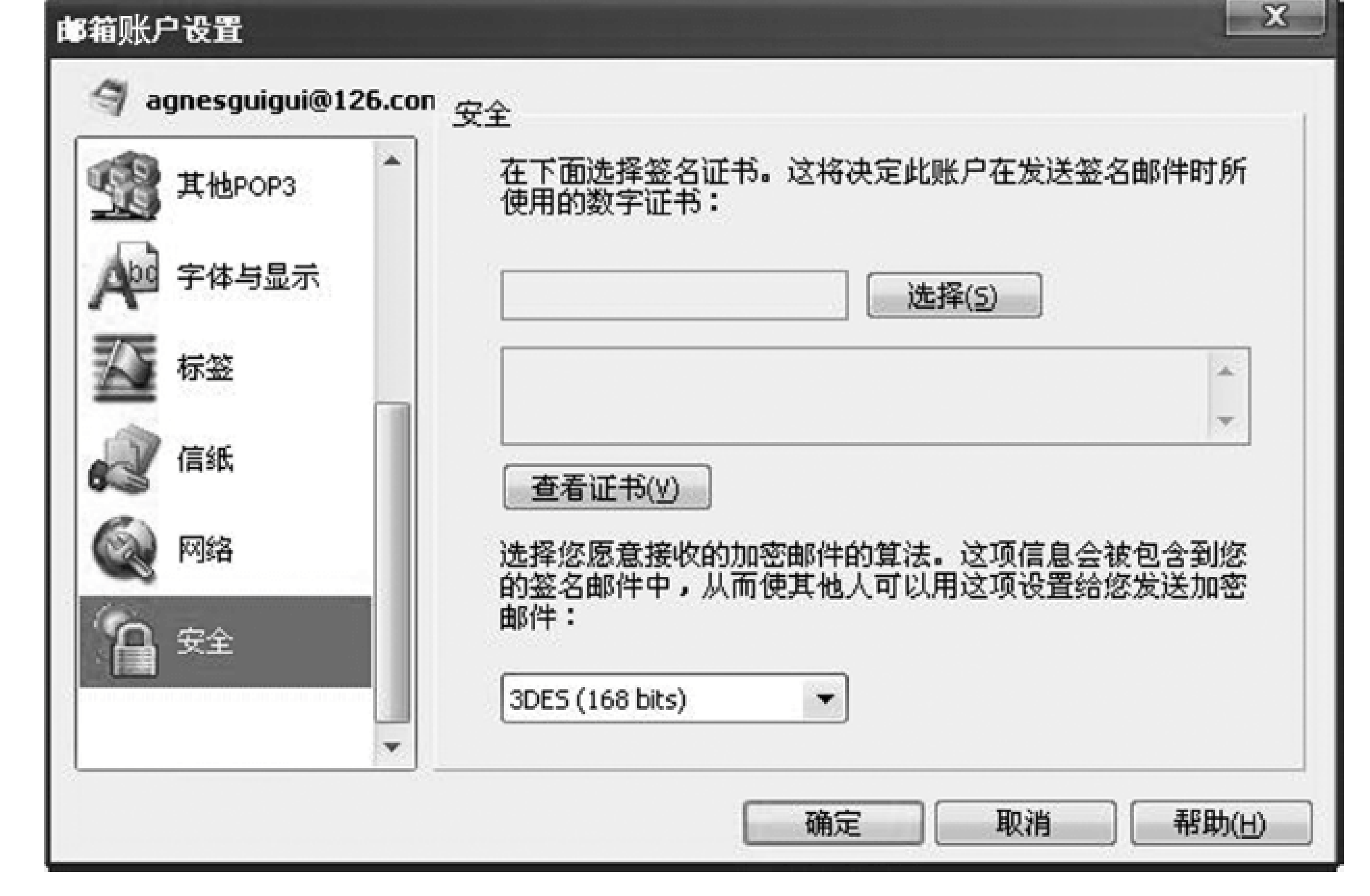


图 8-136 【邮箱账户设置】对话框

(2) 单击【选择】按钮，在弹出的【选择证书】对话框(图 8-137)中，选中 Thawte 证书名称前的复选框并单击【确定】按钮，返回【邮箱账户设置】对话框。

(3) 对话框右侧将显示出证书的相关信息，如图 8-138 所示。单击【确定】按钮，保存邮箱账户设置。

以后在使用 FoxMail 编辑邮件时，即可通过邮件编辑窗口工具栏上的【签名】和【加密】按钮，使用自己的数字证书签名或使用收件人的证书加密邮件。



图 8-137 【选择证书】对话框

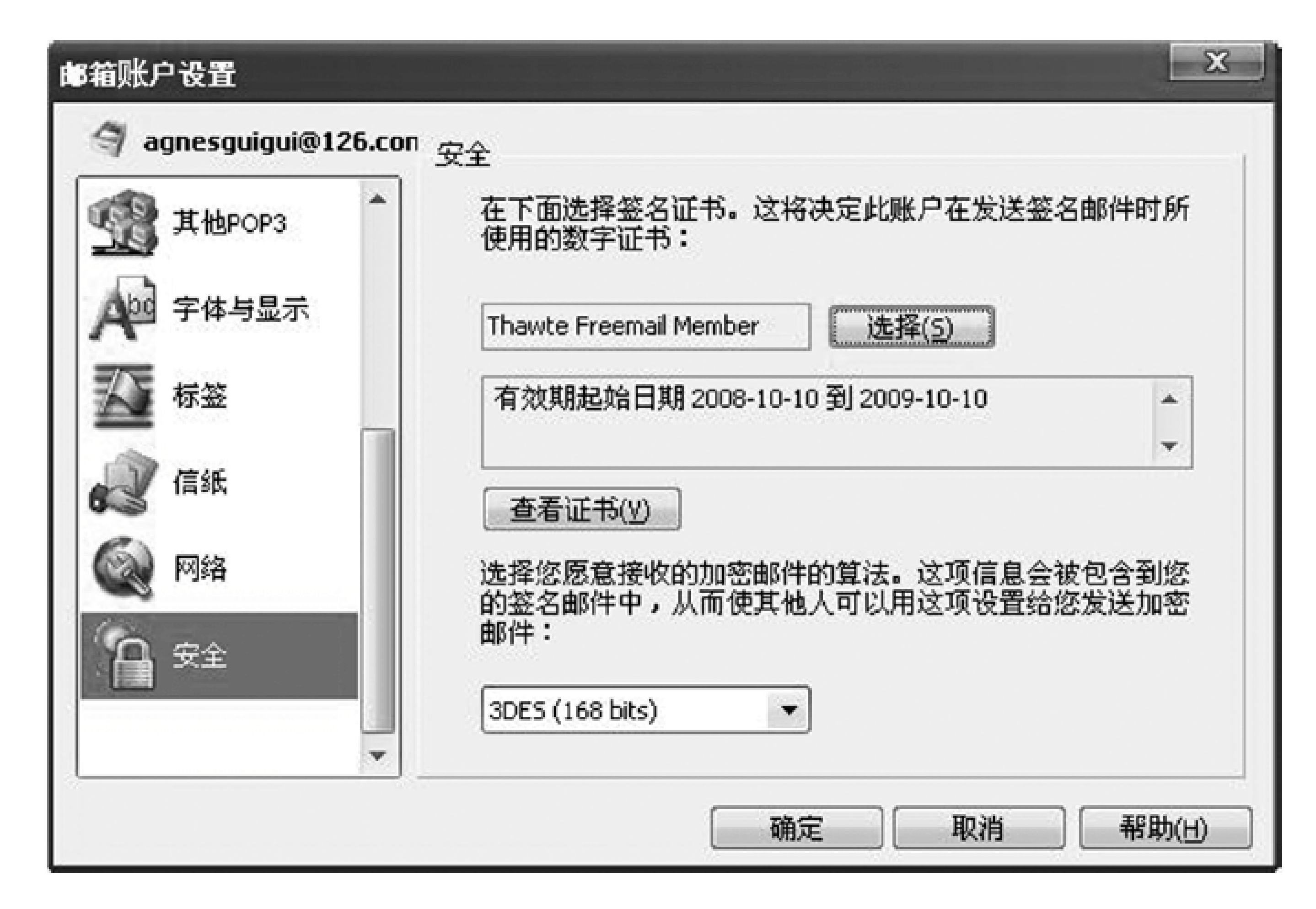


图 8-138 显示出证书相关信息的【邮箱账户设置】对话框

5. 收发安全邮件

在发出的邮件上签名的方法非常简单，在设置邮件客户端软件的过程中，可以选择对所



有发出的邮件签名，也可以设置证书后在编辑邮件时单击【签名】按钮实现签名页面，如图 8-139所示。



图 8-139　单击【签名】按钮实现签名页面

当收件方接到一封已签名或加密的安全邮件时，将分别以不同的图标在“收件箱”中显示使用了数字签名的邮件与加密邮件（验证邮件是否完整和解密的工作将由电子邮件客户端软件自动完成）。在阅读邮件时，软件将首先显示安全邮件帮助页面，邮件可能出现的任何问题都将在该页面上做出详细描述（图 8-140）。单击【继续】按钮，如果该安全邮件存在问题，信息之中可能出现“安全警告”之类的描述，告知用户该邮件已被篡改或并非来自所谓的发件人（图 8-141），告知用户该邮件的数字证书不被信任；如果邮件没有问题，将打开如图 8-142 页面查看邮件内容。

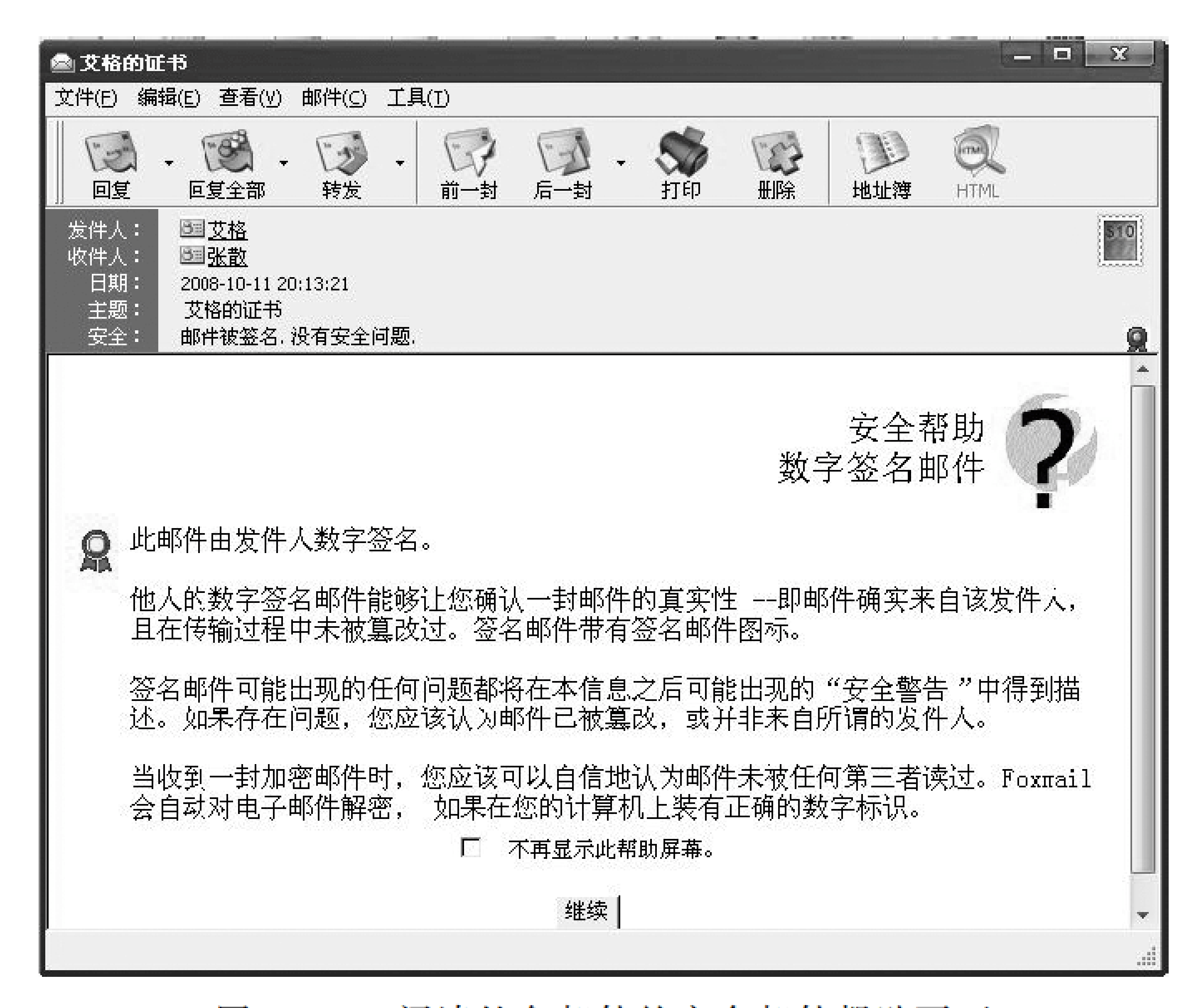


图 8-140　阅读签名邮件的安全邮件帮助页面





图 8-141 安全警告页面



图 8-142 查看邮件内容页面

单击邮件内容窗口右上角的签名图标，可以打开如图 8-143 所示【证书的详细信息】对话框。单击【添加到地址簿】按钮，可以将发件人的证书安装到自己的系统上，以后就可以使用该数字证书对邮件进行加密后发给对方了。

注意：发件人对邮件添加数字签名时，就在邮件中加入了发件人的数字签名和公用密钥。数字签名和公用密钥统称为“证书”。





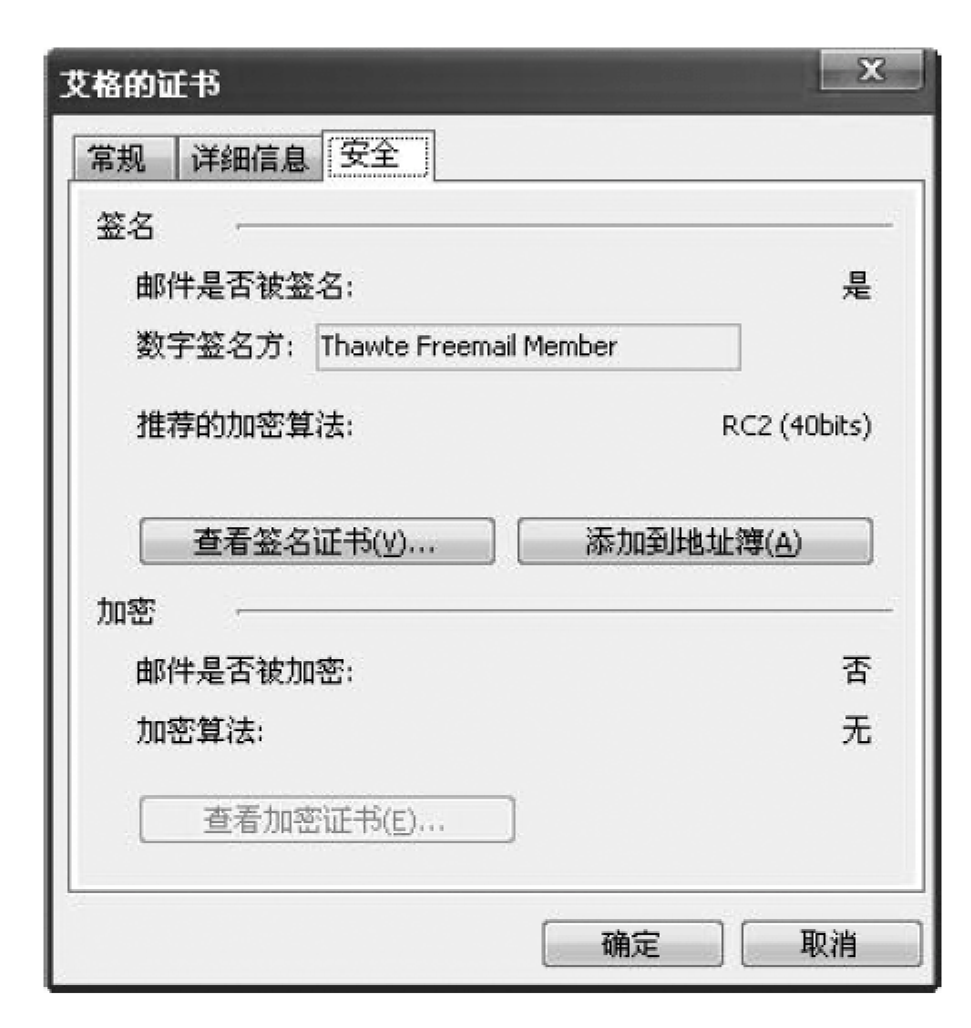


图 8-143　【证书的详细信息】对话框

在阅读加密邮件时，软件将显示安全邮件帮助页面，如图 8-144 所示。单击【继续】按钮，即可查看邮件内容。双击左下角的附件图标，可打开附件。

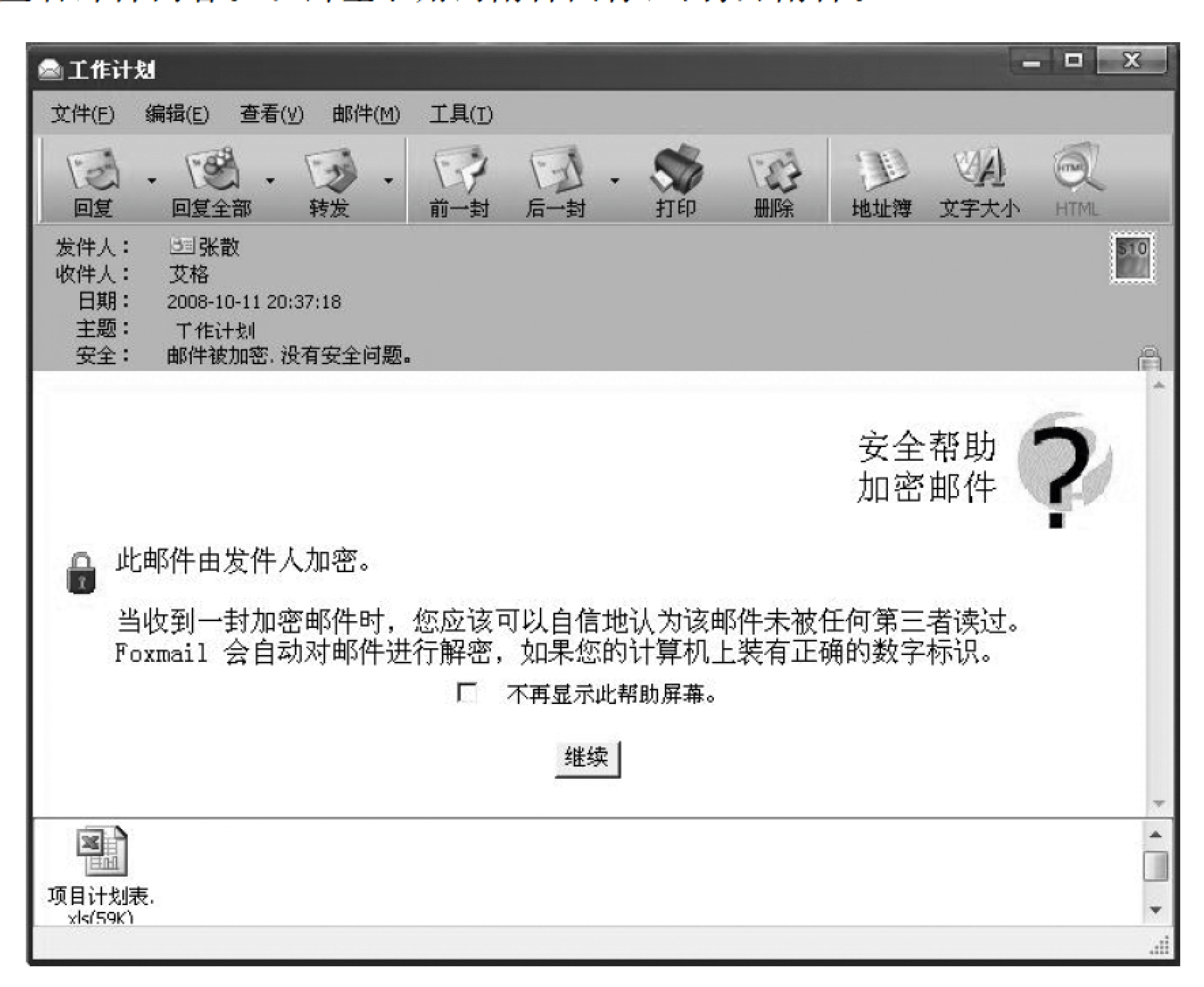


图 8-144　阅读加密邮件的安全邮件帮助页面

6. 证书管理

在自己的计算机上安装了包含私钥的证书后，当接收加密邮件时，解密工作由系统自动完成。如果想在其他计算机上使用该证书，可以通过下面的方法将证书安装到该计算机上。



（1）导出私钥

① 在安装了证书的计算机上，打开 IE 浏览器，选择【工具】/【Internet 选项】命令，弹出如图 8-145 所示【Internet 选项】对话框，选择【内容】选项卡（图 8-146）。



图 8-145 【Internet 选项】对话框



图 8-146 【Internet 选项】的【内容】选项卡

② 在【证书】选项区中单击【证书】按钮，弹出如图 8-147 所示【证书】对话框，单击【导出】按钮，开始导出证书。

③ 在如图 8-148 所示对话框中选择【是，导出私钥】单选按钮，然后连续单击【下一步】按钮，在如图 8-149 所示对话框中输入保护私钥的密码。

④ 单击【下一步】按钮，在如图 8-150 所示对话框中给该私钥取名，并选择存储的位置，即可将私钥导出为一个文件。

（2）导入私钥。在其他计算机上，打开 IE 浏览器，参考导出私钥的操作步骤。不同的是，在如图 8-147 所示【证书】对话框中单击【导入】按钮，随后按提示选择上面导出的证书文件，即可导入证书。



图 8-147 【证书】对话框

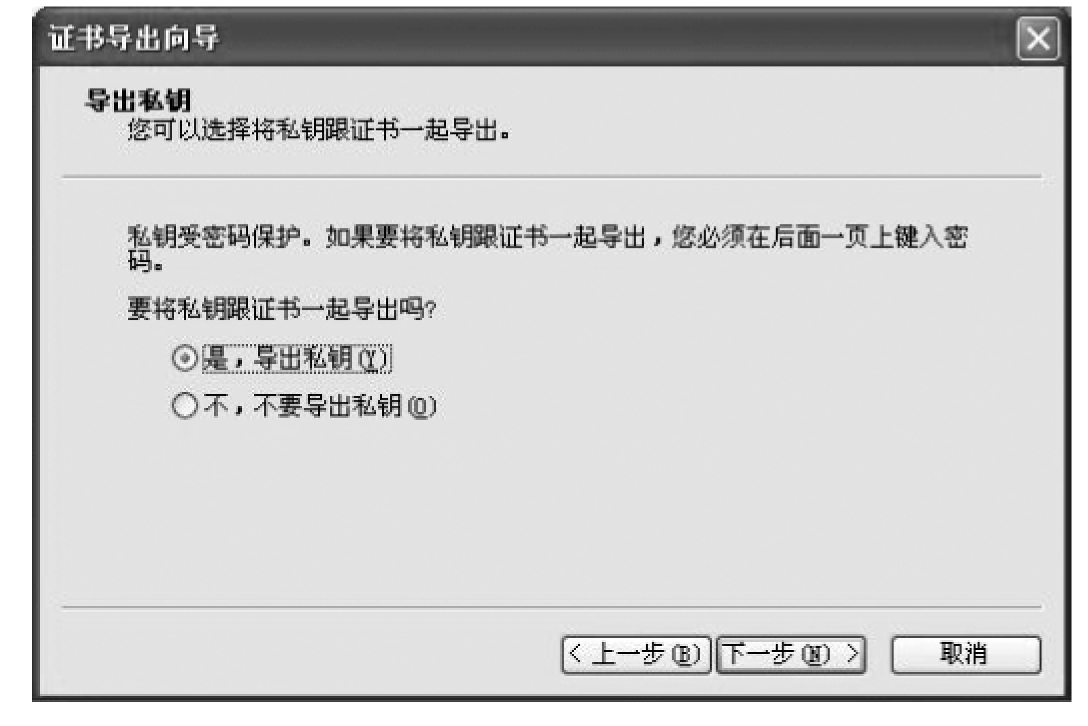


图 8-148 【证书导出向导】对应的【导出私钥】对话框







图 8-149　【证书导出向导】对应的【密码】对话框



图 8-150　【证书导出向导】对应的【要导出的文件】对话框

这样，在该计算机上就可以使用该证书了。对于联系人的电子证书也可以通过同样的方法导出和导入，以便在不同的计算机上仍然可以给对方发送加密邮件。

8.7　习　　题

1. 简述 PKI 技术及其应用。
2. 简述数字证书及其作用。
3. 简述对称密钥算法与非对称密钥算法的异同。
4. 简述 EFS 原理。
5. 密钥的存档与恢复有什么意义？
6. 邮件安全技术包括哪些方面？

第9章　Windows Server 2003安全配置



本章学习目标：

- 理解 NTFS 权限及移动和复制对权限的影响。
- 掌握 NTFS 权限的组合及 AGDLP 规则。
- 能利用 NTFS 权限实现用户和组访问文件夹和文件的安全性。
- 理解本地安全策略、域控制器安全策略和域安全策略。
- 掌握密码策略、账户锁定策略和审核策略。
- 理解组策略作用及应用规则。
- 掌握组策略继承与阻止继承操作。
- 掌握组策略强制生效、筛选组策略设置。
- 掌握利用组策略实现限制软件的执行。

在计算机网络系统管理中，网络服务器的安全管理特别重要，它是整个网络的安全中心。Windows Server 2003 是企业首选的网络操作系统，特别是中小企业。因此，对 Windows Server 2003 进行安全配置非常重要。其安全配置的内容主要包括三个方面：文件权限设置、安全策略配置和组策略配置。

文件权限主要分为共享文件夹权限和 NTFS 权限，本章主要介绍 NTFS 权限的设置。

计算机策略大致分为四类：本地策略、站点策略、域策略和 OU(Organizational Units，组织单位)策略。它们的作用顺序为：本地策略、站点策略、域策略、OU 策略。站点策略一般只在站点之间有慢速连接的时候才会使用，因此，Windows 没有内置站点策略，需要管理员手工设置。本章主要介绍上述策略中的安全策略部分：本地策略中的本地安全策略、域策略中的域安全策略和 OU 策略中的域控制器安全策略。

组策略主要介绍其创建、配置及应用方法。

9.1　文 件 权 限

文件权限使管理员能管理用户对 Windows 计算机上文件系统资源的访问。Windows 是通过设置文件权限来保护数据安全的。文件权限主要有共享文件夹权限和 NTFS 权限等，本章主要介绍 NTFS 权限。

9.1.1　NTFS 权限概述

1. NTFS 概述

NTFS（New Technology File System）是从 Windows NT 开始使用的文件系统，Windows Server 2003 也推荐使用这种高性能的文件系统。它是一个特别为网络和磁盘配额、文件加密等管理安全特性设计的磁盘格式。NTFS 具有如下特点。

(1) 支持更大的磁盘容量。NTFS 可以支持的分区大小可以达到 2TB(即 2048GB)。而 FAT16 文件系统支持分区的大小最大为 4GB，FAT32 文件系统支持分区的大小理论上最大为 2TB。

(2) 设置访问权限。在 NTFS 分区上，可以为共享资源、文件夹和文件设置访问许可权限：一是设置允许访问的组或用户；二是设置其访问的级别。与 FAT32 文件系统下对文件夹或文件进行访问相比，安全性要高得多。

(3) 支持对分区、文件夹和文件的压缩。这种文件系统级的压缩功能效率很高，任何被压缩的内容能被基于 Windows 2000/XP/Server 2003 的应用程序直接读写，不需要解压缩软件。文件关闭或保存时会自动对文件进行压缩。

(4) 支持文件加密。使用 EFS(Encrypting File System，加密文件系统)功能可以对 NTFS 分区上的文件和文件夹进行加密保存。如果没有加密用户的账户和密码，即使是管理员也无法对这些加密资源进行访问。为用户提供了更高层次的安全保证。

(5) 支持数据恢复。NTFS 是一个可恢复的文件系统。NTFS 通过使用标准的事物处理日志和恢复技术来保证分区的一致性。发生系统失败事件时，NTFS 使用日志文件和检查点信息自动恢复文件系统的一致性。

(6) 磁盘配额管理。磁盘配额指管理员可以为用户所能使用的磁盘空间进行配额限制。该功能使管理员可以方便合理地为用户分配存储资源，避免由于磁盘空间使用的失控可能造成的系统崩溃，提高了系统的安全性。

(7) AD 需要使用 NTFS。AD 必须安装在 NTFS 文件系统的分区。

2. 三种文件系统比较

FAT16 文件系统是以前 DOS 使用的文件系统，它最大可以管理 4GB 的分区。

FAT32 文件系统是 FAT16 文件系统的派生文件系统。采用 32 位文件分配表，支持 32GB 的分区。

FAT16、FAT32 和 NTFS 三种文件系统的主要区别如表 9-1 所示。

表 9-1　FAT16、FAT32 和 NTFS 的比较

比较项目	FAT16	FAT32	NTFS
适用操作系统	DOS、Windows 95/98/ME/2000/XP/Server 2003	Windows 95/98/ME/2000/XP/Server 2003	Windows NT/2000/XP/Server 2003
最大分区尺寸	4GB	2TB(理论上)	2TB



续表

比 较 项 目	FAT16	FAT32	NTFS
分区中最多文件数	小于 65 000	接近无限	接近无限
最大文件尺寸	2GB	4GB	决定于文件存放分区的尺寸
最大簇数	65 535	268 435 456	几乎无限
数据压缩支持	不支持	不支持	支持
数据加密支持	不支持	不支持	支持
磁盘配额支持	不支持	不支持	支持
安全性构造	不支持	不支持	支持
可恢复性	不支持	不支持	支持
磁盘空间节约	在大分区上最低	一般	最大

3．怎样获得 NTFS

(1) 格式化磁盘时选择 NTFS。格式化磁盘时，可以在文件系统的下拉列表框中选择 NTFS(图 9-1)。

(2) 将 FAT 分区转换为 NTFS 分区。使用 convert 命令可以将 FAT 分区无损转换为 NTFS 分区，但 NTFS 分区无法转换为 FAT 分区。例如，将 D 盘转换为 NTFS 格式，则在非 D 盘输入命令：convert d:/fs:ntfs。

(3) 使用软件进行转换。可以使用第三方软件(如 PQmagic)将 FAT 分区转换为 NTFS 分区。



图 9-1 格式化磁盘对话框

4．NTFS 权限

NTFS 权限是指系统管理员或文件拥有者赋予用户和组访问某个文件和文件夹的权限，通过允许或禁止某些用户或组访问文件或文件夹，实现对资源的保护。NTFS 权限既可以在本地应用，也可以在域中应用。

NTFS 权限分为 NTFS 文件权限和 NTFS 文件夹权限。NTFS 文件权限是应用在文件上的 NTFS 权限，用来控制用户对文件的访问。NTFS 文件夹权限用来控制用户对文件夹和该文件夹下的文件及子文件夹的访问。默认该文件夹下的文件及子文件夹继承该文件夹的 NTFS 权限，因此，通过对文件夹设置权限可以赋予该文件夹下的文件及子文件夹权限。

表 9-2 列出了 NTFS 文件权限和 NTFS 文件夹权限基本类型的内容。

表 9-2 中的权限可以称之为 NTFS 的标准权限。除了这几种标准权限外，还有一些特殊的 NTFS 权限，作为这几种标准权限的补充和细化。例如，在特殊 NTFS 权限中把标准权限中的“读取”权限细分为“读取数据”、“读取属性”、“读取扩展属性”和“读取权限”四种更加具体的权限。NTFS 特殊权限与标准权限的关系如表 9-3 所示。



表 9-2　NTFS 文件权限和 NTFS 文件夹权限基本类型

权限类型	NTFS 文件权限	NTFS 文件夹权限
读取	允许用户读取文件，查看文件的属性、所有者及其权限	允许用户查看文件夹内的文件和子文件夹的属性、所有者及其权限
写入	允许改写文件，改变文件的属性，查看文件的所有者及其权限	允许用户在文件夹中创建新文件和子文件夹，改变文件夹的属性，查看文件夹的所有者及其权限
列出文件夹内容	无此选项	允许用户查看文件夹内的文件和子文件夹的内容
读取和运行	允许用户运行应用程序，执行读取权限操作	允许用户把文件夹移动到其他文件夹中（即使用户没有其他文件夹的权限），执行读取权限，执行列出文件夹内容操作
修改	允许用户修改或删除文件，执行写入权限，执行读取和运行权限	允许用户修改或删除文件夹，执行写入权限，执行读取和运行权限
完全控制	允许用户修改文件 NTFS 权限并获得文件所有权，允许用户执行修改权限	允许用户修改文件夹 NTFS 权限并获得文件夹所有权、删除子文件夹和文件的 NTFS 权限，允许用户执行其他所有权限

表 9-3　NTFS 特殊权限与标准权限的关系

标准 NTFS 权限 / 特殊 NTFS 权限	完全控制	修改	读取和运行	列出文件夹内容	写入	读取
完全控制	√					
遍历文件夹/运行文件	√	√	√			√
列出文件夹/读取数据	√	√	√	√		√
读取属性	√	√	√	√		√
读取扩展属性	√	√	√	√		√
创建文件/写入数据	√	√			√	
创建文件夹/附加数据	√	√			√	
写入属性	√	√			√	
写入扩展属性	√	√			√	
删除子文件夹及文件	√					
删除	√	√				
读取权限	√	√	√	√		√
更改权限	√					
取得所有权	√					



9.1.2 NTFS 权限规则

一个用户可能同时属于多个组,而不同的组对某个文件夹或文件拥有不同的权限,那么该用户对该文件夹或文件具有怎样的权限呢?对于这种多重权限,NTFS 遵循以下的规则分配用户权限的优先级。

1. 权限的累加

用户对某文件夹或文件的有效权限是分配给该用户和该用户所属所有组权限的总和。例如,用户 stu002 同时属于组 stua 和 office02,三者对某文件的权限分别为读取、写入和运行。那么,该用户拥有的有效权限为三个权限的总和:读取+写入+运行。

2. 文件权限高于文件夹权限

如果某用户拥有对某文件及其所在文件夹不同的权限,则文件的权限高于文件夹的权限。例如,用户 stu002 拥有对文件夹 C:\Tools 写入的权限,同时拥有对文件 C:\Tools\mylx.txt 读取的权限,那么该用户对文件 C:\Tools\mylx.txt 拥有的有效权限为读取权限。

3. 拒绝权限高于其他权限

如果用户对某文件夹或文件同时拥有"拒绝权限"和其他权限时,拒绝权限高于其他权限,即该用户的有效权限为拒绝权限。拒绝权限可以赋予用户,也可以赋予组。例如,用户 stu001 同时属于组 stua 和 stub,三者对某文件的权限分别为读取、写入和拒绝写入。那么,该用户拥有的有效权限为读取权限。虽然组 stua 对该文件拥有写入权限,但组 stub 对该文件拥有拒绝写入权限,拒绝权限高于其他权限,因此,组 stua 赋予 stu001 的写入权限不生效。

4. 权限的继承

默认情况下,新建的子文件夹和文件会继承父文件夹的权限,根目录下的文件或文件夹继承磁盘分区的权限。如果要拒绝继承父文件夹权限可以通过相关操作实现,如果要强制下级继承也可以通过相关操作实现。如果一个文件拒绝继承父文件夹权限,然后又设置其父文件夹强制下级继承,那么,该文件被强制继承其父文件夹的权限,即后来设置的权限覆盖前面设置的权限(详细操作在 9.2 节中介绍)。

5. 复制和移动对权限的影响

对于 NTFS 分区上的文件,从一个文件夹复制或移动到另一个文件夹后,其 NTFS 权限会发生变化。如果 NTFS 分区上的文件或文件夹被复制或移动 FAT 分区中,由于 FAT 分区没有权限设置,原来的权限全部消失。复制和移动文件权限的变化如表 9-4 所示。此操作要求操作者必须拥有对目的文件夹的写入权限。

表 9-4 复制和移动文件权限的变化

分　区	复　制	移　动
同一 NTFS 分区	继承目的地文件夹的权限	保留原来的权限
不同 NTFS 分区	继承目的地文件夹的权限	继承目的地文件夹的权限
NTFS 分区→FAT 分区	权限消失	权限消失

6. AGDLP 规则

A 表示用户账号,G 表示全局组,DL 表示本地域组,P 表示资源权限。A-G-DL-P 策略是将用户账户添加到全局组中,将全局组添加到本地域组中,然后为本地域组分配资源权限。其作用通过如下实例说明。

网络系统中存在两个域 stua 和 teacha,stua 域中的用户(stu001 和 stu002)和 teacha 域中的用户(teach001 和 teach002)都需要访问 teacha 域中的文件夹 data。设置的方法有两种。

方法一:在 teacha 中建一个 DL,因为 DL 的成员可以来自所有的域,然后把这 4 人都加入这个 DL,并把 data 的访问权限赋给 DL。

这样设置虽然可以实现访问权限要求。但存在如下缺点:DL 存在于 teacha 域中,其管理权也在 teacha 域,如果 stua 域中还有其他人需要访问 data,stua 域管理员是无权做修改的,只能通知 teacha 域管理员,让他对 DL 的成员做修改。如果需要访问 data 的域有 3 个甚至更多,怎么办?全部修改都要由 teacha 域管理员来完成,这种设置太麻烦了。

方法二:在 stua 和 teacha 域中都各建立一个全局组(Gstu 和 Gteach),stua 域管理员将 stu001 和 stu002 加入 Gstu,teacha 域管理员将 teach001 和 teach002 加入 Gteach,然后在 teacha 域中建立一个 DL,把这两个全局组都加入 teacha 域中的 DL 中,然后把 data 的访问权赋给 DL。

这样,通过组的权限继承,两个全局组都有权限访问文件夹 data 了。由于两个全局组分布在 stua 和 teacha 域中,因此,域管理员可以分别管理自己的全局组。以后有任何修改,都可以自己设置,不用麻烦 teacha 域的管理员了。

9.2 NTFS 权限设置

设置 NTFS 权限就是对文件或文件夹设置用户访问的权限,包括设置文件权限、设置文件夹权限、设置 NTFS 特殊权限、拒绝继承权限、强迫继承权限等。

9.2.1 设置文件夹的 NTFS 权限

对于指定的文件夹,只有其拥有者、管理员和有完全控制权限的用户才可以设置其 NTFS 权限。下面通过实例说明这样的用户怎样将该文件夹的相关权限赋予其他用户。例如设置 stua 组的用户 stu001 对文件夹 C:\Tools 拥有“写入”权限。详细操作步骤如下:

(1) 以 Administrator 账户登录系统(建议采用 Windows Server 2003 R2 EnterPrise Edition),在 teach.com 域中建立两个用户账户(如 stu001 和 stu002)和一个组(如 stua),设



置这两个账户隶属于 stua 组。在 Tools 文件夹上右击，在弹出的快捷菜单中选择【属性】命令，在打开的【Tools 属性】对话框中选择【安全】选项卡（图 9-2）。

（2）单击【添加】按钮，打开【选择用户、计算机或组】对话框，单击【高级】按钮，在打开的对话框中单击【立即查找】按钮（图 9-3），在搜索结果文本框中找到用户 stu001，选择该用户（图 9-4），单击【确定】按钮，选择的用户名 stu001 出现在【输入对象名称来选择】列表框中（图 9-5）。



图 9-2 【Tools 属性】对话框的【安全】选项卡



图 9-3 【选择用户、计算机或组】对话框的【高级】选项



图 9-4 选择用户 stu001



（3）单击【确定】按钮，返回【Tools 属性】对话框，在【stu001 的权限】列表框中选中“写入”选项对应的【允许】复选框（图 9-6），单击【确定】按钮。完成权限的设置。



图 9-5　stu001 出现在【输入对象名称来选择】列表框中

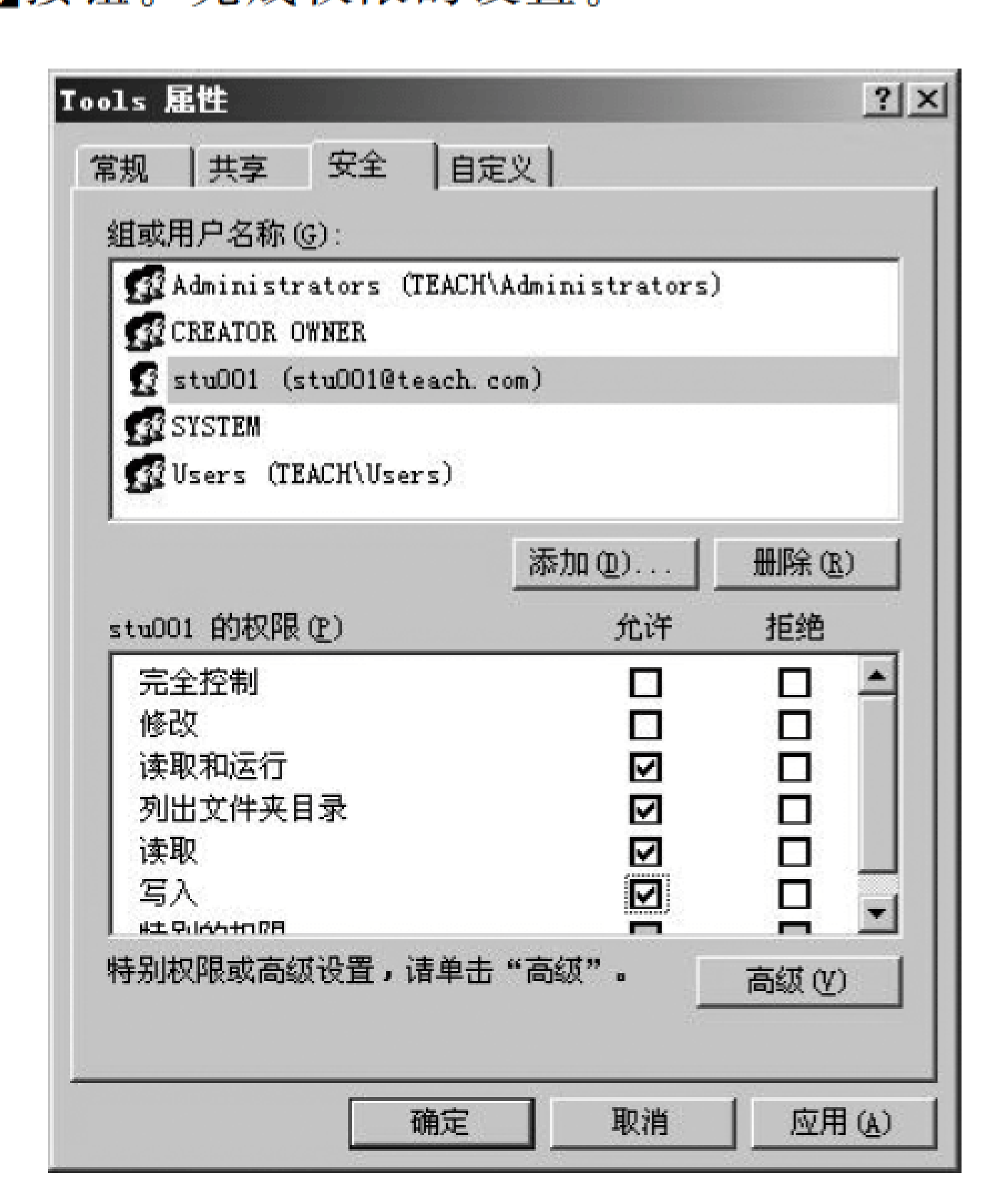


图 9-6　【stu001 的权限】列表框

（4）注销 Administrator 账户，以 stu001 账户登录系统，在文件夹 C:\Tools 中新建文件，验证设置是否成功。在文件夹 C:\Tools\remain 中新建文件，验证权限的继承。

9.2.2　设置文件的 NTFS 权限

对于指定的文件，只有其拥有者、管理员和有完全控制权限的用户才可以设置其 NTFS 权限。例如设置 stua 组的用户 stu002 对 C:\Tools\mylx.txt 文件拥有“修改”权限。详细操作步骤如下：

（1）以 Administrator 账户登录系统（建议采用 Windows Server 2003 R2 EnterPrise Edition）。在 mylx.txt 文件上右击，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择【安全】选项卡（图 9-7）。

（2）单击【添加】按钮，打开【选择用户、计算机或组】对话框。单击【高级】按钮，在打开的对话框中单击【立即查找】按钮（图 9-3），在搜索结果文本框中找到用户 stu002，选择该用户。单击【确定】按钮，选择的用户名 stu002 出现在【输入对象名称来选择】列表框中（图 9-8）。

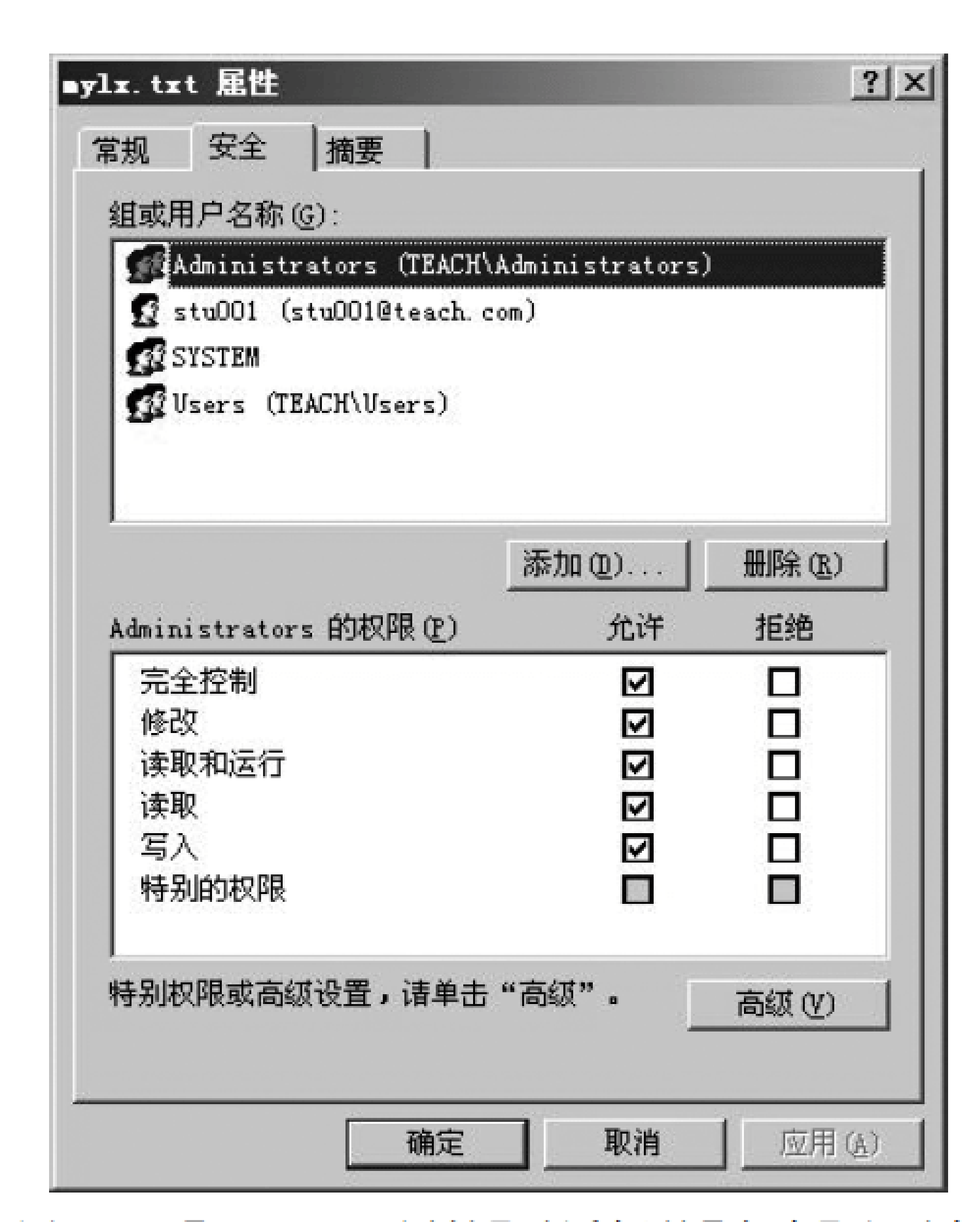


图 9-7　【mylx.txt 属性】对话框的【安全】选项卡



(3) 单击【确定】按钮,返回【Tools 属性】对话框,在【stu002 的权限】列表框中选中"修改"选项对应的【允许】复选框(图 9-9),单击【确定】按钮。完成权限的设置。



图 9-8 stu002 出现在【输入对象名称来选择】列表框中

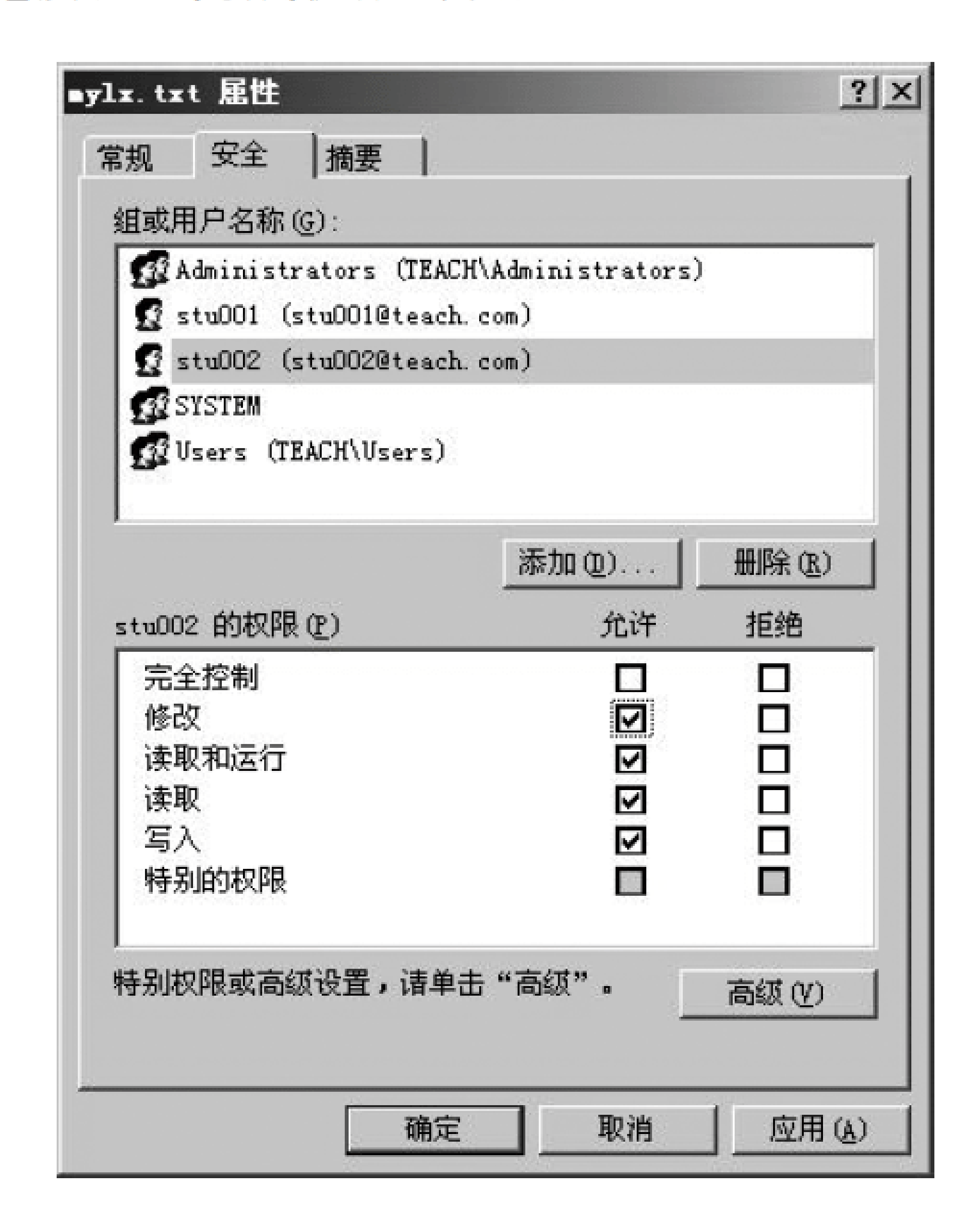


图 9-9 【stu002 的权限】列表框

(4) 注销 Administrator 账户,以 stu002 账户登录系统,对 C:\Tools\mylx.txt 文件进行修改并保存,以验证设置是否成功。

9.2.3 设置 NTFS 特殊权限

NTFS 特殊权限及其与 NTFS 标准权限的关系如表 9-3 所示。

在特殊权限中有两个较难理解的权限:更改权限和取得所有权。

1. 更改权限

在标准 NTFS 权限中,只有"完全控制"权限才允许用户拥有更改文件或文件夹的权限,但是,"完全控制"权限同时拥有删除子文件夹或文件的权限。如果要赋予一个用户更改文件或文件夹的权限,又不能让其删除子文件夹和文件,这时就要用到特殊权限中的"更改权限"。例如设置用户 stu002 对文件 C:\Tools\mylx.txt 拥有更改权限。

详细的操作步骤是:以 Administrator 账户登录系统(建议采用 Windows Server 2003 R2 EnterPrise Edition)。在图 9-9 所示的对话框中单击【高级】按钮,在打开的【mylx.txt 高级安全设置】对话框的【权限项目】列表框中选择用户 stu002(图 9-10)。然后单击【编辑】按钮,在打开的【mylx.txt 的权限项目】对话框的【权限】列表框中选中【更改权限】复选框(图 9-11)。单击【确定】按钮,返回上一级对话框,多次单击【确定】按钮,直到关闭全部对话框。完成权限的设置。

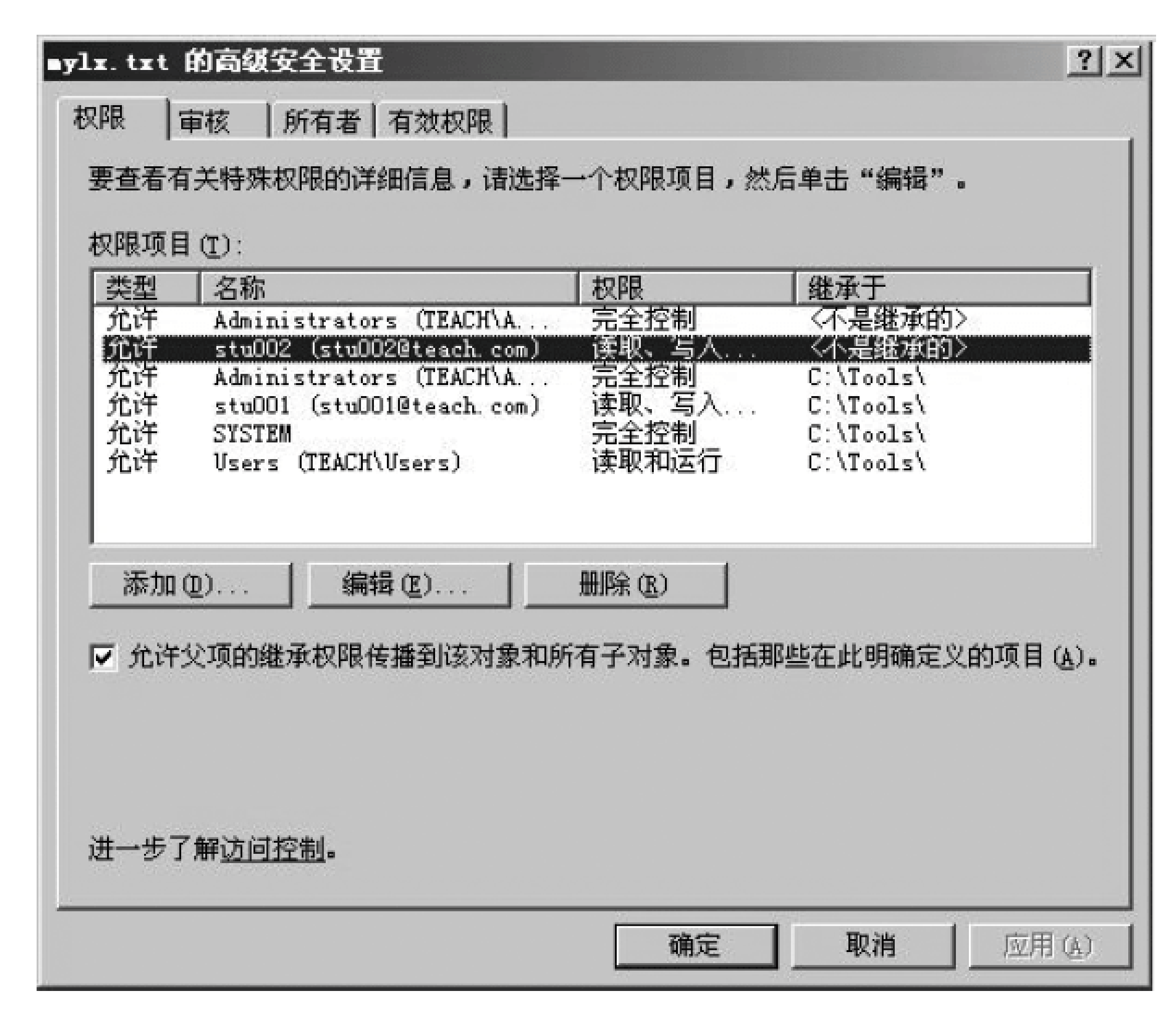



图 9-10 【mylx.txt 高级安全设置】对话框

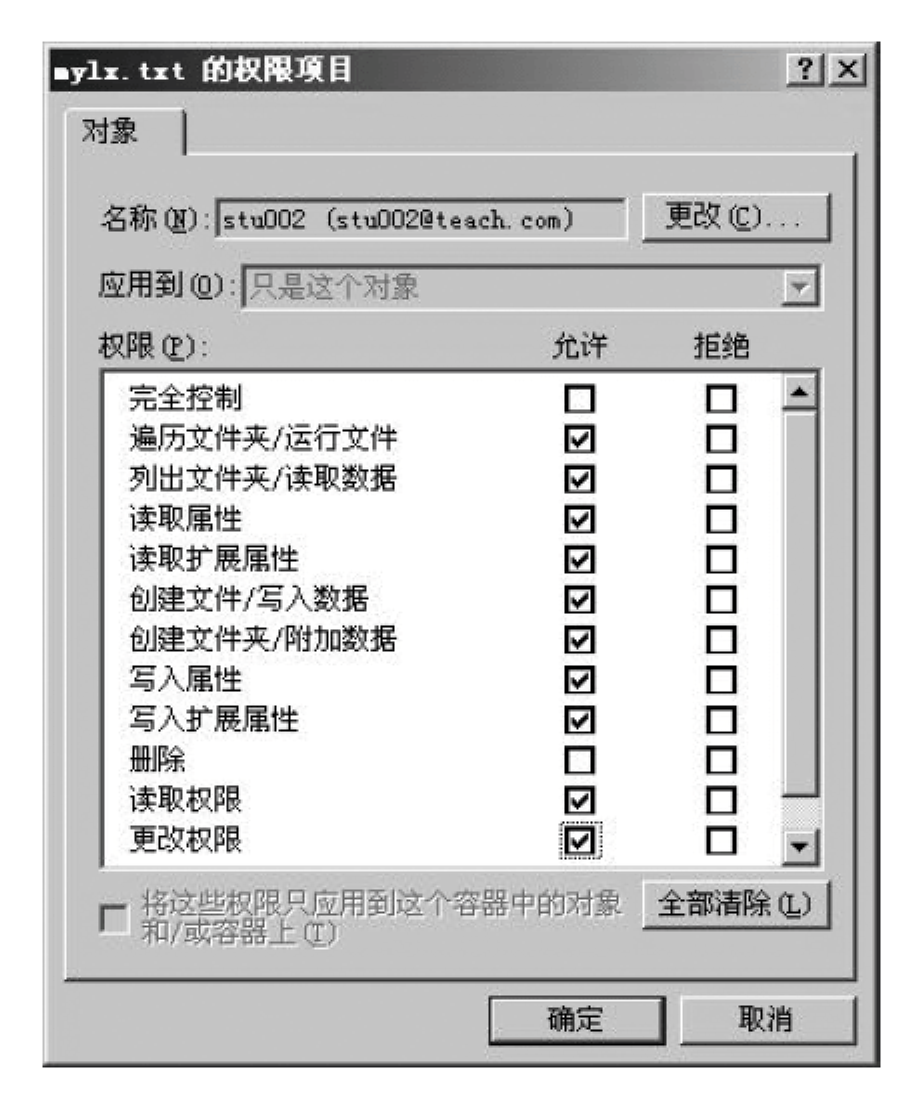


图 9-11 【mylx.txt 的权限项目】对话框

2. 取得所有权

由于各种指派和撤销权限操作，可能会造成所有用户(包括管理员)都无法访问某个文件夹或文件的情况。这时就要用到特殊权限中的“取得所有权”。

默认情况下，文件夹或文件的创建者(即所有者)拥有对该文件夹或文件的所有权。取得所有权的用户才能够指派权限。取得所有权有以下两种方式。

- 文件夹或文件的所有者将“取得所有权”赋予别的用户。
- 管理员可以取得所有权(但不能转让所有权给别的用户)。

如何让管理员取得所有权呢？以取得由用户 stu001 创建的 C:\Tools\stu001_lx.txt 文件的所有权为例。详细步骤说明如下：

(1) 以 Administrator 账户登录系统。在 C:\Tools\stu001_lx.txt 上右击，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择【安全】选项卡。

(2) 单击【高级】按钮，在打开的【stu001_lx.txt 的高级安全设置】对话框中选择【所有者】选项卡，可以看到【目前该项目的所有者】文本框中显示的所有者为 stu001。在【将所有者更改为】列表框中选择 Administrators(图 9-12)，单击【确定】按钮。返回上一级对话框，单击【确定】按钮，关闭所有对话框。即完成权限设置。

(3) 重新查看该文件属性，按照上述相同的步骤操作，在打开的【stu001_lx.txt 的高级安全设置】对话框中选择【所有者】选项卡，可以看到【目前该项目的所有者】文本框中显示的所有者为 Administrators(图 9-13)。说明 Administrators 成功地取得了该文件的所有权。

9.2.4 拒绝继承权限和强制继承权限

父文件夹拥有的权限默认被子文件夹及包含在父文件夹中的其他文件继承。当用户修改某文件夹的权限时，同时也改变了该文件夹包含的子文件夹和文件的权限。





图 9-12 【stu001_lx.txt 的高级安全设置】对话框



图 9-13 所有权改变后的【stu001_lx.txt 的高级安全设置】对话框

1. 拒绝继承权限

如果不想继承父文件夹的权限，可以通过下面的操作实现。例如拒绝文件夹 C:\Tools\remain 继承 C:\Tools 的权限。详细操作步骤如下：

(1) 以 Administrator 账户登录，右击 C:\Tools\remain 文件夹，在打开的【remain 属性】对话框中，选择【安全】选项卡。单击【高级】按钮，打开【remain 的高级安全设置】对话框(图 9-14)，取消默认选中的【允许父项的继承权限传播到该对象和所有子对象。包括那些在此明确定义的项目】复选框。



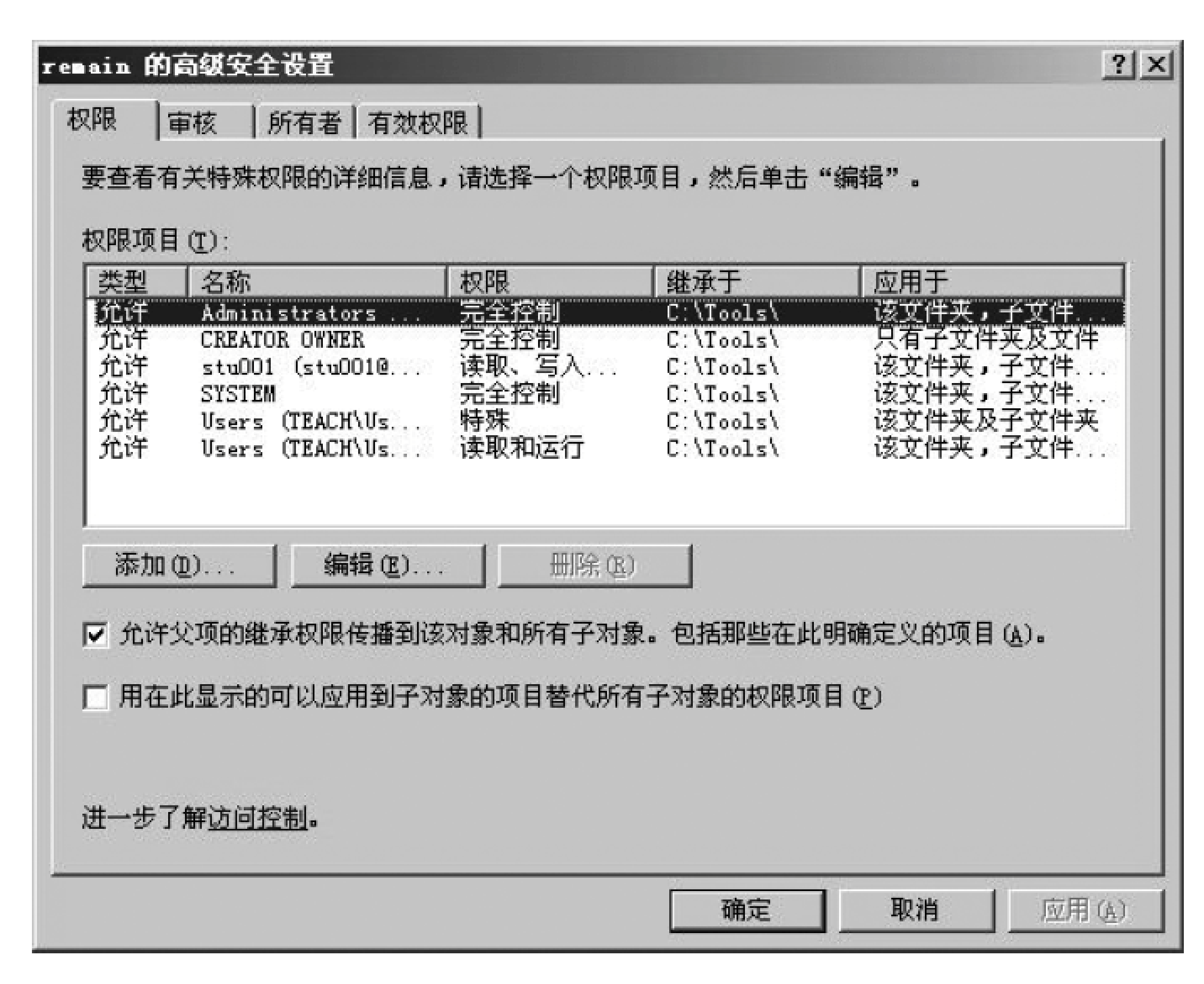


图 9-14　【remain 的高级安全设置】对话框

（2）弹出【安全】对话框，单击【删除】按钮。返回上一级对话框，可以看到【权限项目】文本框中所有继承的权限全部被清空（图 9-15）。

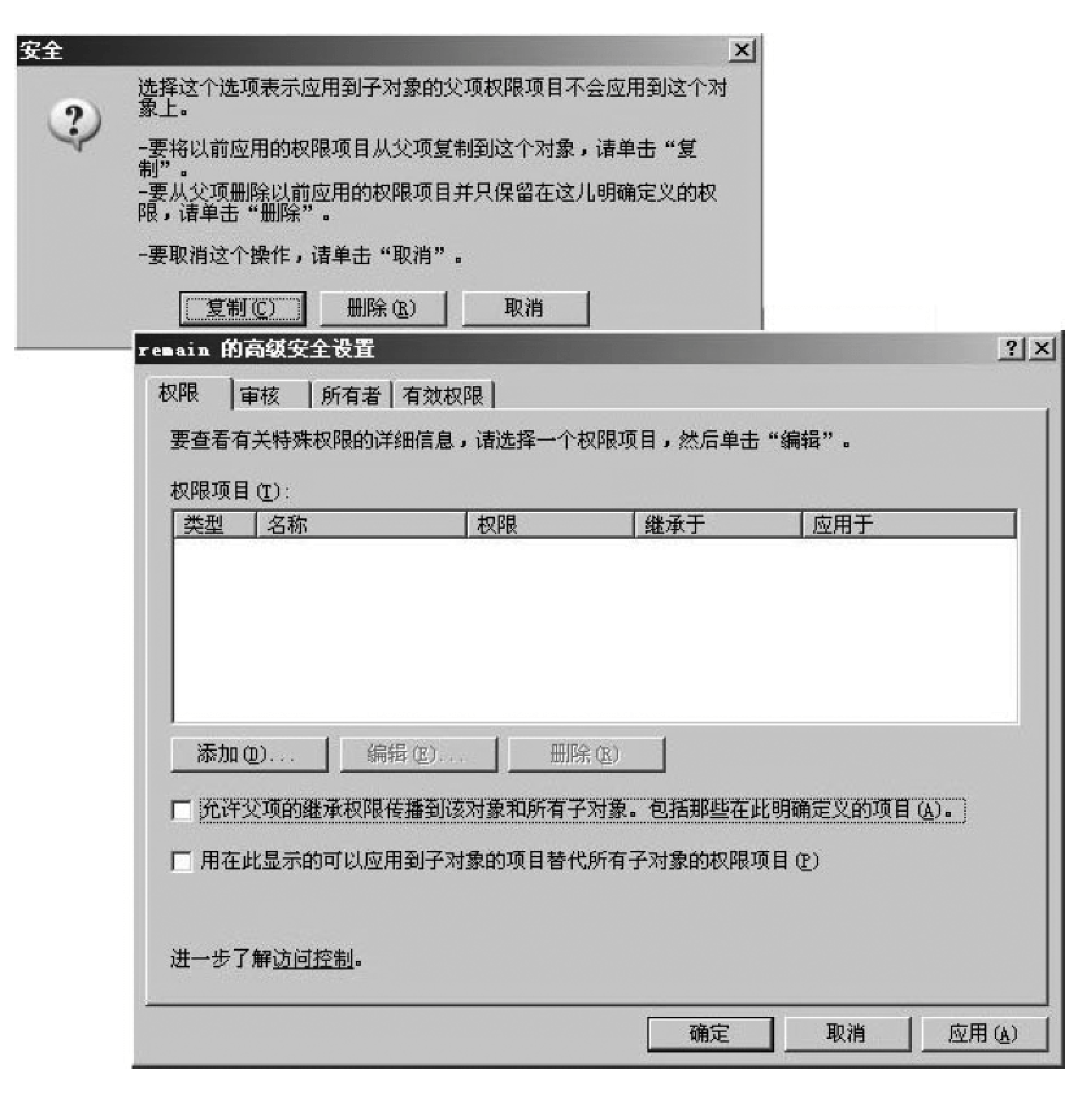


图 9-15　【安全】对话框



(3) 此时，切记要单击【添加】按钮，然后参考前面的“设置文件夹的 NTFS 权限”步骤，添加一些用户对该文件夹的访问权限(例如，添加 Administrator 账户对其拥有“完全控制”权限)。否则没有人能访问它，只有所有者才能更改权限。

(4) 注销 Administrator 账户，以 stu001 账户登录，验证该账户是否拥有对文件夹 C:\Tools\remain 的写入权限。

提示：根据前面的权限设置，stu001 账户拥有对文件夹 C:\Tools 的写入权限，根据权限继承原则，该账户也拥有对文件夹 C:\Tools\remain 的写入权限。但是，通过拒绝继承权限设置，只有 Administrator 账户拥有对文件夹 C:\Tools\remain 的访问权限。因此，stu001 账户无法对该文件夹进行任何访问操作。

2. 强制继承权限

如果要强制下级继承权限，可以通过下面的操作实现。例如强制文件夹 C:\Tools 的子文件夹及文件继承 C:\Tools 的权限。详细步骤如下：

(1) 以 Administrator 账户登录，参考前面的步骤，单击图 9-2 对话框中的【高级】按钮，打开【Tools 的高级安全设置】对话框，选中【用在此显示的可以应用到子对象的项目替代所有子对象的权限项目】复选框(图 9-16)。

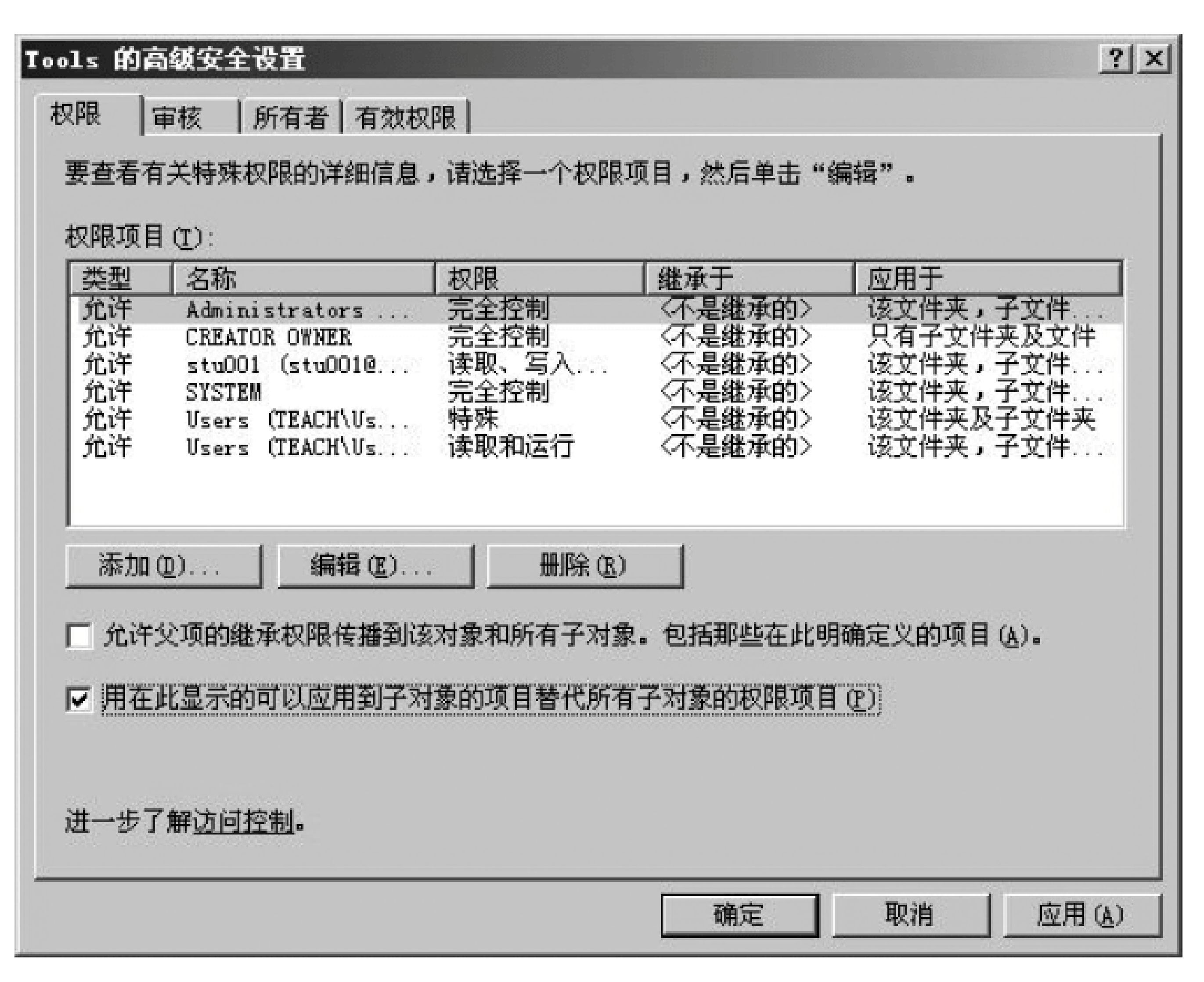


图 9-16 【Tools 的高级安全设置】对话框

(2) 单击【确定】按钮，弹出【安全】对话框(图 9-17)，提示该操作将删除子对象的明确定义过的权限(即强制下级继承，删除下级原来的权限)，单击【是】按钮。返回上一级对话框，单击【确定】按钮，关闭所有对话框，完成强制继承权限。

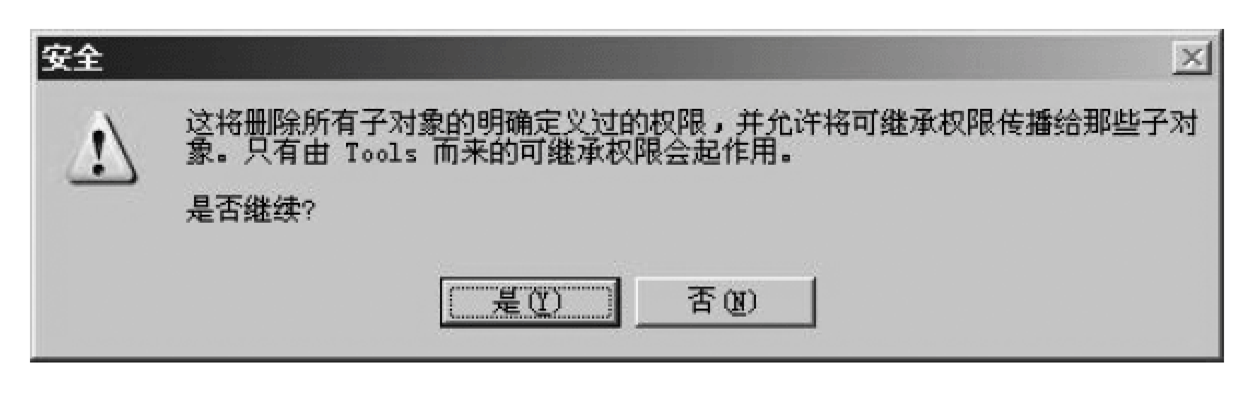


图 9-17 【安全】对话框



(3) 验证。参考前面的步骤，重新打开【remain 的高级安全设置】对话框，发现其【权限项目】文本框中的设置恢复到拒绝继承权限之前的设置(图 9-14)，说明该文件夹被强制继承权限了。为了进一步验证，可以再次以 stu001 账户登录，验证该账户是否拥有对文件夹 C:\Tools\remain 的写入权限。

注意： 设置文件夹 C:\Tools\remain 拒绝继承权限，然后设置其父文件夹 C:\Tools 强制下级继承权限，则文件 C:\Tools\remain 原来设置的拒绝权限失效，继承其父文件夹的权限，即后来设置的权限覆盖前面设置的权限。反之，先设置强制继承权限，再设置拒绝权限，则拒绝继承权限覆盖强制继承权限。

9.3　利用 AGDLP 规则设置 NTFS 权限

9.3.1　案例背景及方案设计

1. 案例背景

某公司的信息处(2 人)和销售处(3 人)人员需要对 alldata 文件夹有读取和写入的权限，而其他处室人员对该文件夹只有读取的权限。

2. 方案设计

根据公司要求，设计方案如下。

(1) 在安装 Windows Server 2003 R2 EnterPrise Edition 操作系统的计算机上进行下面的权限设置操作。

(2) 创建 2 个全局组和 1 个本地域组。

(3) 每个全局组中按人员数创建用户账户。

(4) 将 2 个全局组加入本地域组(设名为 loca)。

(5) 为本地域组设置对 alldata 文件夹的读取和写入权限。

(6) 创建其他组用户账户，设置对 alldata 文件夹的读取权限。

(7) 全局组、其他组及相应用户账户设置如表 9-5 所示。

表 9-5　全局组、其他组及相应用户账户设置

全局组名称	用户账户名称	对文件夹 alldata 拥有的权限
info	info001、info002	读取和写入
sale	sale001、sale002、sale003	读取和写入
other	other001、other002	读取

9.3.2　NTFS 权限设置步骤

(1) 根据表 9-5 创建全局组(info 和 sale)及相关用户账户，并将相关用户加入各全



局组。

(2) 创建本地域组(loca),并将全局组(info 和 sale)加入本地域组。结果大致如图 9-18 所示。

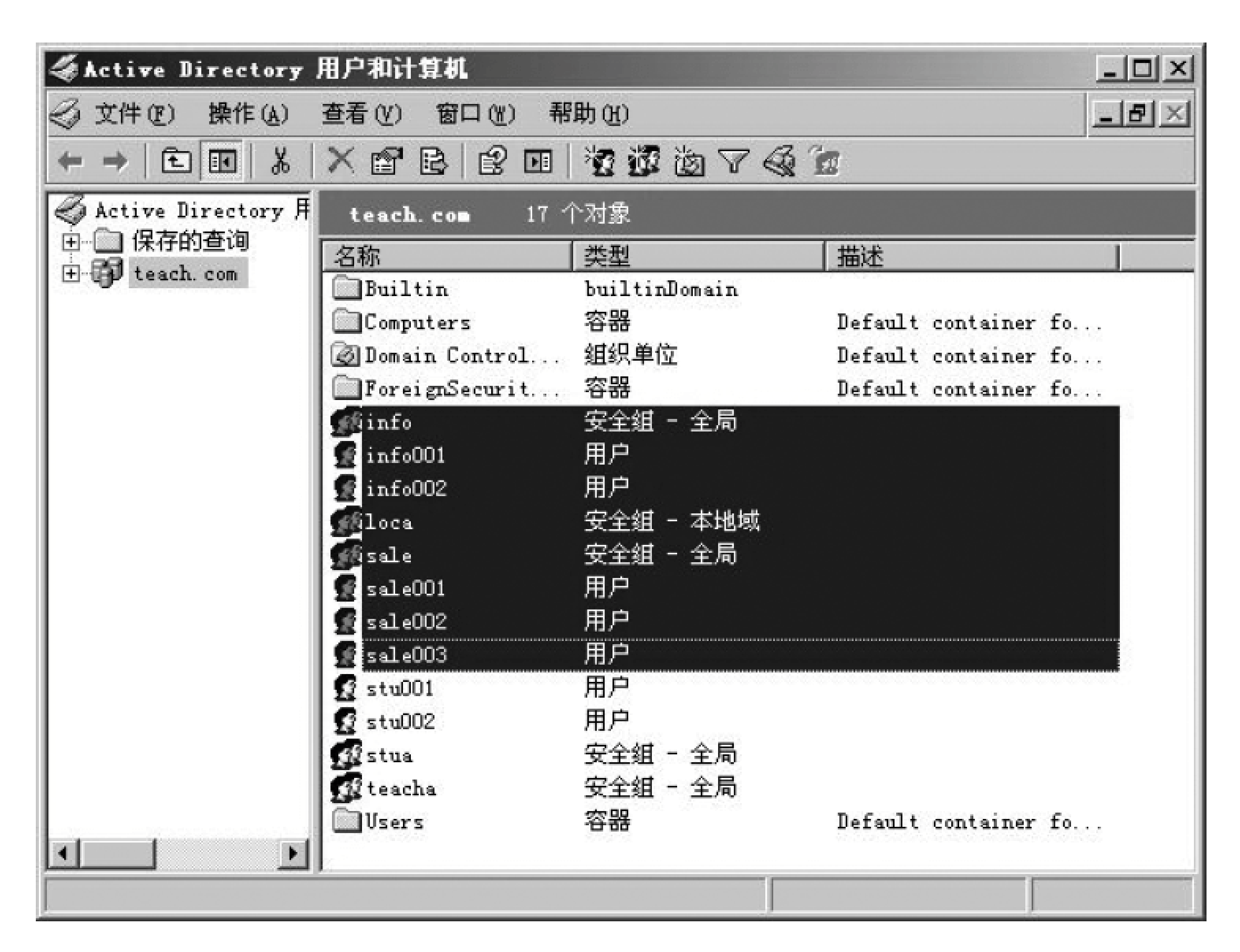


图 9-18 【Active Directory 用户和计算机】窗口

(3) 创建其他组(other),并将其他用户加入该组。

(4) 为本地域组(loca)设置对 alldata 文件夹的读取和写入权限。详细步骤参考 9.2.1 小节,结果如图 9-19 所示。

(5) 为其他组(other)设置对 alldata 文件夹的读取权限。详细步骤参考 9.2.1 小节,结果如图 9-20 所示。



图 9-19 【alldata 属性】对话框的 loca 的权限



图 9-20 【alldata 属性】对话框的 other 的权限





9.4　本地安全策略

本地安全策略是 Windows 2000/XP/Server 2003 系统自带的系统安全管理工具，通过设置本地安全策略可以大大提高系统的安全性。本地安全策略主要包括账户策略和本地策略。如果将一台服务器升级为域控制器(安装了 AD)，则在域控制器中，本地安全策略被域控制器安全策略代替，同时增加了可以控制整个域安全的域安全策略。

9.4.1　账户策略

用户账户的安全主要通过设置密码进行保护。为了避免用户身份由于密码被破解而被夺取或盗用，通常可采取如提高密码的破解难度、启用账户锁定策略、限制用户登录、限制外部连接以及防范网络嗅探等措施。

账户策略中包括了密码策略和用账锁定策略。

1. 密码策略

密码策略通过强制提高密码复杂性、增大密码长度、提高更换频率等措施来提高密码的破解难度。包括如下 6 个策略：密码必须符合复杂性要求、密码长度最小值、密码最长使用期限、密码最短使用期限、强制密码历史、用可还原的加密来存储密码。

设置密码策略的方法如下：选择【开始】/【程序】/【管理工具】/【本地安全策略】命令，打开【本地安全设置】窗口(图 9-21)，在左侧窗口的目录树中，选择【账户策略】/【密码策略】选项，打开如图 9-22 所示的【密码策略】属性窗口，在右侧详细信息列表窗格中显示可配置的密码策略选项的当前配置。因为各策略选项的配置方法基本一样，所以在此仅以第一个选项的配置进行介绍，其他只对各选项的具体作用进行简单介绍。



图 9-21　【本地安全设置】窗口

注意：如果在【开始】/【程序】选项中没有找到【管理工具】选项，可以通过【控制面板】打开【管理工具】选项。



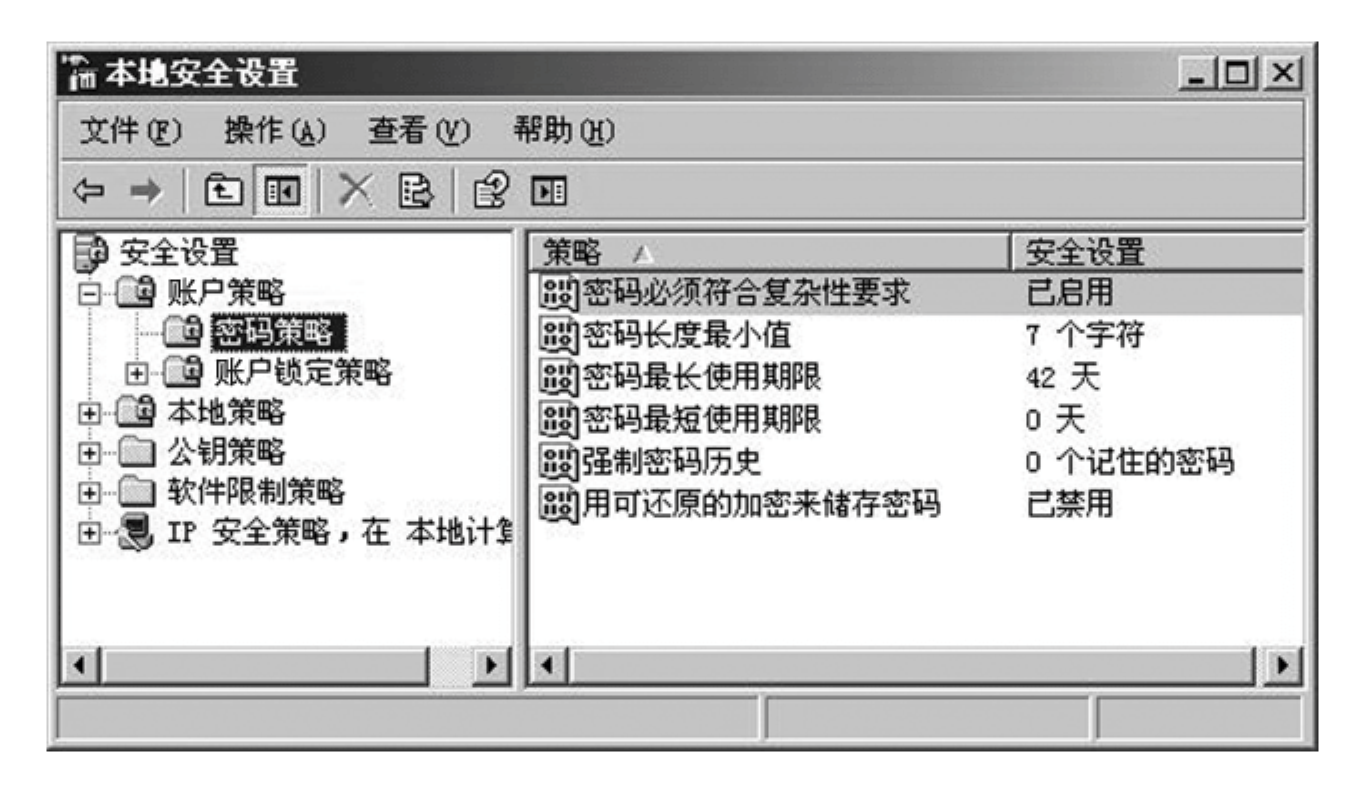


图 9-22　【密码策略】属性窗口

(1) 密码必须符合复杂性要求。此策略确定密码是否必须符合一系列被认为是对于强密码来说很重要的规则。默认情况下，该策略在域控制器上启用，在独立服务器上禁用。

配置方法是：在如图 9-22 所示的右侧详细信息列表窗格中，双击【密码必须符合复杂性要求】选项，打开【密码必须符合复杂性要求 属性】对话框(图 9-23)。在默认选择的【本地安全设置】选项卡中，通过选择【已启用】或【已禁用】单选按钮，启用或禁用该策略。关于该策略的详细解释，可以通过选择【解释这个设置】选项卡进行查看(图 9-24)。

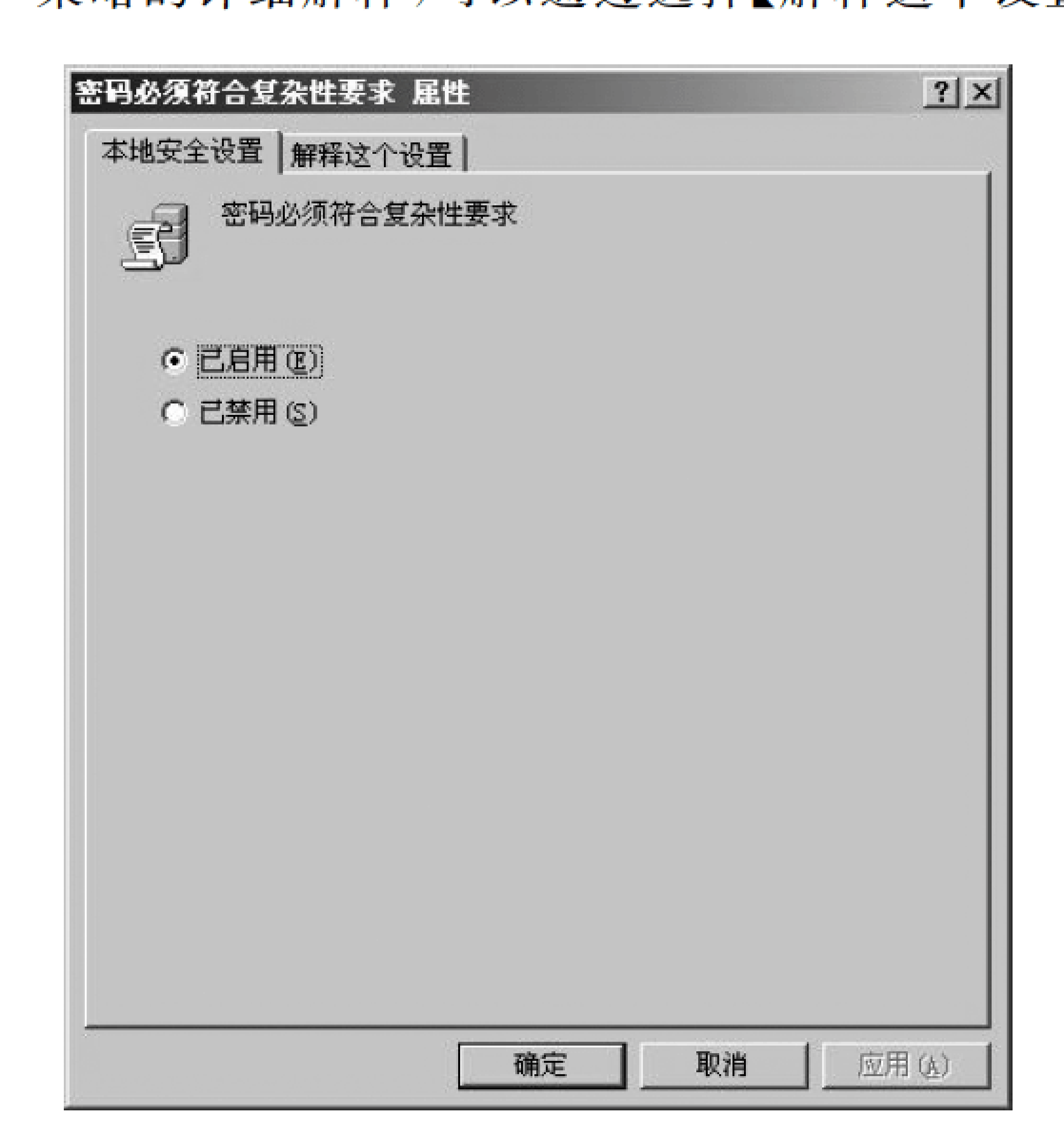


图 9-23　【本地安全设置】选项卡

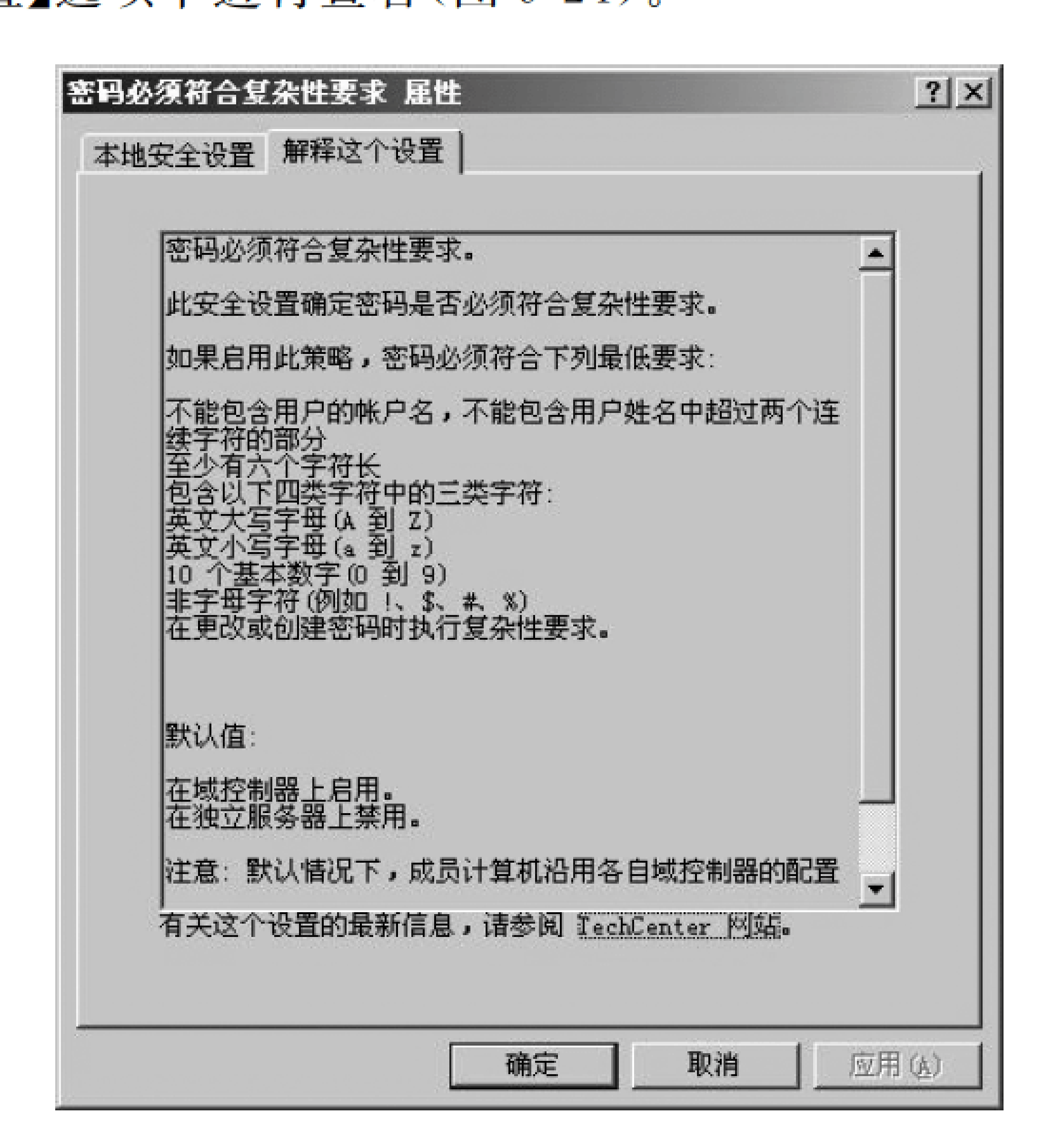


图 9-24　【解释这个设置】选项卡

注意：选择右侧详细信息列表窗格中的策略选项进行设置有两种方法，一是双击相应策略选项；二是在相应选项上右击，在弹出的快捷菜单上选择【属性】选项。以下选择策略选项进行设置的方法相同，不再重复。

如果启用此策略设置，密码必须符合以下要求。

- 密码长度至少有 6 个字符。
- 密码包含下列四类字符中的三类：大写字符(A、B、C、…)；小写字符(a、b、c、…)；数



字(0、1、2、3、4、5、6、7、8、9);非字母数字字符和 Unicode 字符(( )`～！ @ ＃ $ % ^ & * － + = | \ { } [ ]：;"'< >，. ? / € Γ ƒ λ 以及空格)

注意：如果启用了此安全策略，当所配置的用户密码不符合此配置要求时系统会提示错误。通常人们设置密码只用数字和字母，没有考虑到字母的大小写或者非字母数字字符，达不到复杂性要求。更改或创建密码时，会强制执行复杂性要求。

(2) 密码长度最小值。此策略设置确定用户账户的密码必须至少由几个字符构成。密码长度最小值的数值可以设置在 1～14 之间，或者将字符数设置为 0(即不需要密码)。默认情况下，该策略在域控制器上值为 7，在独立服务器上值为 0。

(3) 密码最长使用期限。此策略设置用户在必须更改密码之前可使用该密码的天数。其值为 0～999 之间，值为 0 时密码永不过期，但不建议使用这种配置。

如果密码最长使用期限设置为 0，则密码最短使用期限可以是 0～998 之间的任意值。建议设置为 30～90 天后过期。

注意：任何密码，甚至最复杂的密码，都可能会被有足够的时间和计算机处理能力的攻击者猜测(或者“破译”)出来。下列某些策略设置可使密码在一个合理的时间段内较难被破译。如果经常要求用户更改其密码，可降低有效密码被破译的风险，还可降低以不正当手段获取密码的人员未经授权登录的风险。使密码每隔 30～90 天过期一次是一种安全最佳操作。

(4) 密码最短使用期限。该策略确定在允许用户更改密码之前必须使用该密码的天数。其值必须小于“密码最长使用期限”值。可以设置为 1～998 之间的某个值，如果设置为 0，则允许立即更改密码。默认情况下，该策略在域控制器上设置为 1，在独立服务器上设置为 0。

(5) 强制密码历史。通过设置该策略确保旧密码不能继续使用，从而增强安全性。默认情况下，该策略在域控制器上设置为 24，在独立服务器上设置为 0。

注意：密码重用对于任何组织来说都是需要考虑的重要问题。许多用户都希望在很长时间以后使用或重用相同的账户密码。特定账户使用相同密码的时间越长，攻击者能够通过强力攻击确定密码的机会就越大。此外，任何可能已被破坏的账户，只要其密码没有更改，就将一直可被利用。如果要求更改密码但仍在重用密码，或者用户不断重用少数几个密码，则好的密码策略的有效性将会大大降低。

(6) 用可还原的加密来存储密码。此策略确定在存储密码时是否使用可还原的加密来存储密码，默认设置为禁用。

如果组织通过远程访问或 Internet 身份认证服务(Internet Authentication Service，IAS)使用身份验证协议(Challenge Handshake Authentication Protocol，CHAP)，或在 IIS 中使用摘要式身份验证，则必须将此策略设置为“已启用”。将此设置逐个用户应用到组策略是异常危险的，因为它需要相应用户账户对象在 Microsoft 管理控制台(MMC) Active Directory 用户和计算机管理单元中打开。

注意：请永远不要启用此策略设置，除非业务要求比保护密码信息更为重要。



2. 账户锁定策略

账户锁定策略是指在某些情况下(如账户受到采用密码词典或暴力破解方式的在线自动登录攻击等),为确保该账户的安全而将此账户进行锁定,使其在一定时间内不能再次使用此账户,从而挫败连续的猜解尝试。包含三个策略:账户锁定阈值、账户锁定时间、复位账户锁定计数器。

在如图 9-21 所示的左侧窗口的目录树中,选择【账户策略】/【账户锁定策略】选项(图 9-25),参照(1)即可对相应策略进行设置。各策略含义如下:

(1) 账户锁定阈值。该策略设置确定导致用户账户被锁定的登录失败尝试次数。在管理员手动解锁或账户锁定时间到达之前,不能使用已锁定的账户。登录失败尝试次数范围为 0～999 之间。如果设置为 0 ,将永不锁定账户,则账户锁定时间和复位账户锁定计数器安全设置显示为"不适用",即不用设置(图 9-25)。默认设置为 0。

注意:"账户锁定策略"在策略默认状态下是被禁用的,从网络安全角度考虑,为防止黑客的恶意攻击,建议并启用该策略,并进行合理设置,建议"账户锁定阈值"为 3。

(2) 账户锁定时间。该策略在账户锁定阈值设置不为 0 时启用。账户锁定时间指无效登录次数达到账户锁定阈值时,锁定账户的时间,范围为 0～99999 分钟。如果将"账户锁定时间"设置为 0,则账户一直保持锁定状态,直到管理员手动将其解锁。"账户锁定时间"必须大于或等于复位时间。

(3) 复位账户锁定计数器。该策略在账户锁定阈值设置不为 0 时启用。复位账户锁定计数器指在无效登录次数未达到账户锁定阈值之前,重新复位登录次数需要的时间,范围为 0～99 999 分钟。如果设置为 0,则账户一直保持锁定状态,直到管理员手动将其解锁。

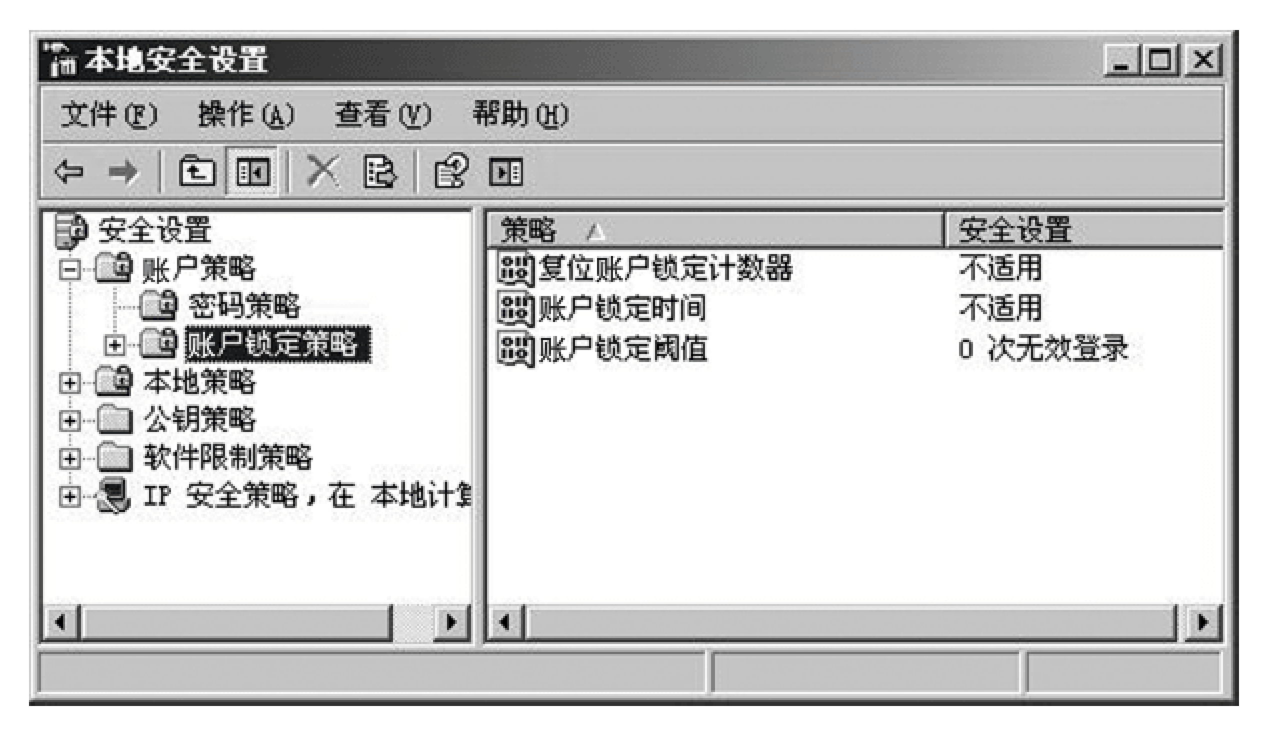


图 9-25 【账户锁定策略】属性窗口

9.4.2 本地策略

本地策略包括审核策略、用户权限分配和安全选项。

1. 审核策略

系统审核机制可以对系统中的各类事件进行跟踪记录并写入日志文件,以供管理员进





行分析、查找系统和应用程序故障及各类安全事件。包括以下九个策略选项：审核账户登录事件、审核策略更改、审核登录事件、审核对象访问、审核过程跟踪、审核目录服务访问、审核特权使用、审核系统事件、审核账户管理。

设置审核策略的方法如下：在如图 9-21 所示的左侧窗口的目录树中，选择【本地策略】/【审核策略】选项，打开如图 9-26 所示的【审核策略】属性窗口，在右侧详细信息列表窗格中显示可配置的审核策略选项的当前配置。因为各策略选项的配置方法基本一样，所以在此仅以【审核账户登录事件】选项的配置进行介绍，其他只对各选项的具体作用进行简单介绍。



图 9-26　【审核策略】属性窗口

(1) 审核账户登录事件。该策略确定是否审核当系统验证账户身份时，用户登录或注销的每个事件。在本地计算机上对本地用户进行身份验证时，该事件记录在本地安全日志中。

在如图 9-26 所示的右侧详细信息列表窗格中，双击【审核账户登录事件】选项，在默认打开的【审核账户登录事件 属性】对话框的【本地安全设置】选项卡中，可以选中【成功】和【失败】复选框(图 9-27)。那么当某个账户登录成功或失败时，将产生成功或失败审核项。也可以不选择，将不对该事件进行相应的审核。默认设置为审核成功。关于该策略的详细解释可以通过选择【解释这个设置】选项卡进行查看。

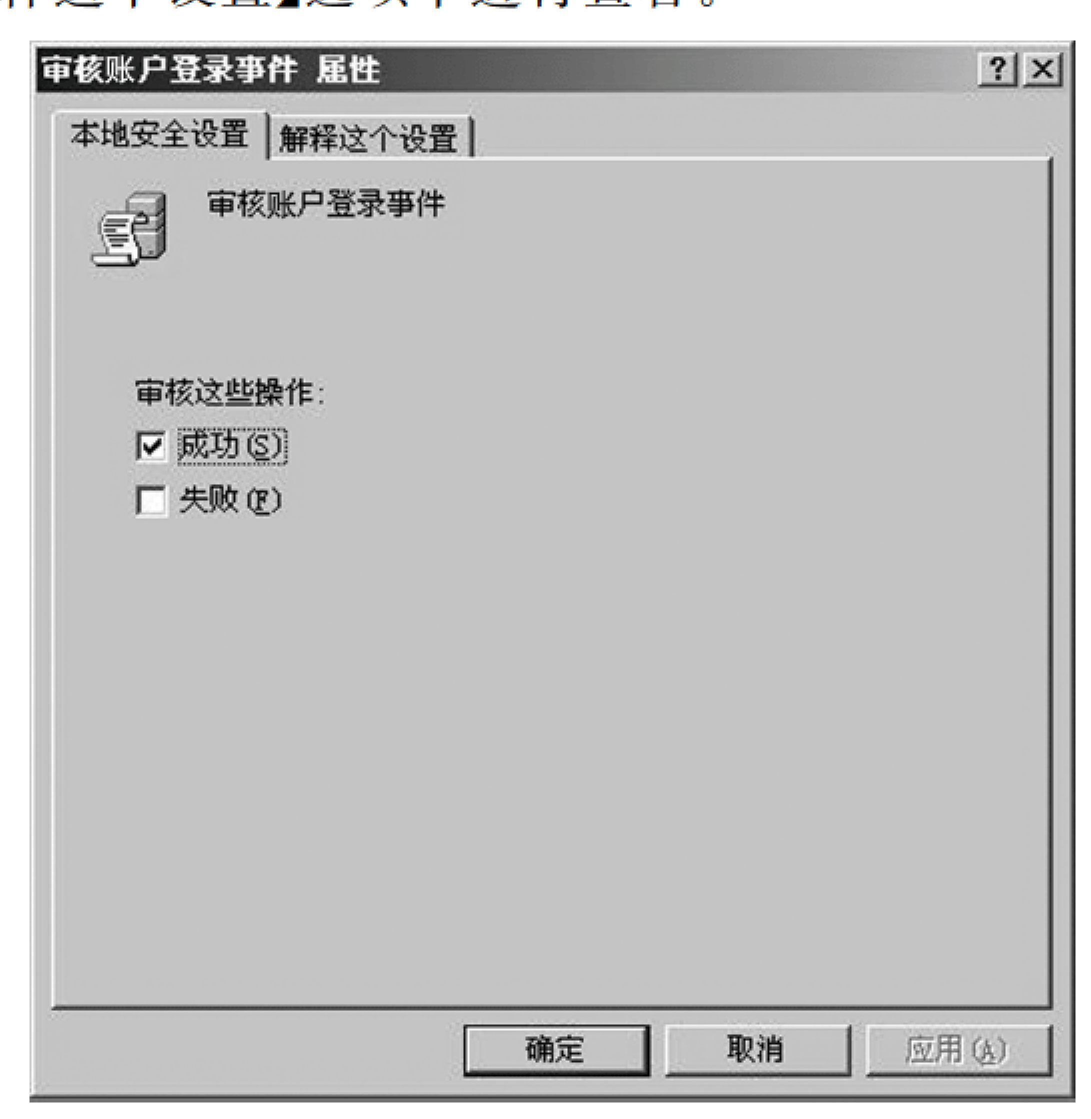


图 9-27　【本地安全设置】选项卡



（2）审核策略更改。该策略确定是否对用户权限分配策略、审核策略或信任策略更改的每一个事件进行成功或失败审核。默认情况下，在域控制器上设置为“成功”，在成员服务器上设置为“无审核”。

（3）审核登录事件。该策略确定是否对每一个登录或注销计算机的用户事件进行成功或失败审核。默认设置为审核成功。

（4）审核对象访问。该策略确定是否对用户访问某个对象（如文件、文件夹、注册表项、打印机等，它们都有自己特定的 SACL）的事件进行成功或失败审核。默认设置为无审核。

（5）审核过程跟踪。该策略确定是否对事件（如程序激活、进程退出、句柄复制和间接对象访问等）的详细跟踪信息进行成功或失败审核。默认设置为无审核。

（6）审核目录服务访问。该策略确定是否对用户访问那些指定自己的系统访问控制列表（System Access Control List，SACL）的 Active Directory 对象的事件进行成功或失败审核。默认情况下，在域控制器上设置为“成功”，在成员服务器上设置为“未定义”。

（7）审核特权使用。该策略确定是否对用户实施其用户权利的每一个事件进行成功或失败审核。默认设置为无审核。

（8）审核系统事件。当用户重新启动或关闭计算机时，或者对系统安全或安全日志有影响的事件发生时，该策略确定是否予以成功或失败审核。默认情况下，在域控制器上设置为“成功”，在成员服务器上设置为“无审核”。

（9）审核账户管理。该策略确定是否对计算机上的每个账户管理事件进行成功或失败审核。账户管理事件的示例包括：

- 创建、修改或删除用户账户或组。
- 重命名、禁用或启用用户账户。
- 设置或修改密码。

默认情况下，在域控制器上设置为“成功”，在成员服务器上设置为“无审核”。

注意：推荐的审核策略为：账户登录事件（进行成功和失败审核）；账户管理（进行成功和失败审核）；目录服务访问（只进行失败审核）；登录事件（进行成功和失败审核）；对象访问（只进行失败审核）；策略更改（进行成功和失败审核）；特权使用（只进行失败审核）；系统事件（进行成功和失败审核）。

2. 用户权限分配

用户权限是允许用户在计算机系统或域中执行的任务。其权限选项包括从网络访问此计算机、从远程系统强制关机、更改系统时间、关闭系统、拒绝本地登录、拒绝从网络访问这台计算机、允许在本地登录等约 39 项。

在图 9-21 所示的左侧窗口的目录树中，选择【本地策略】/【用户权限分配】选项，打开如图 9-28 所示的【用户权限分配】属性窗口。在右侧详细信息列表窗格中显示可配置的安全选项的当前配置。

下面只对几个常用的策略选项作介绍，其他策略选项可以根据需要参考下列的方法进行设置。

（1）从网络访问此计算机。该用户权限确定允许哪些用户和组通过网络连接到该计算



图 9-28　【用户权限分配】属性窗口

机。此用户权限不影响终端服务。

在如图 9-28 所示的右侧详细信息列表窗格中，双击【从网络访问此计算机】选项，打开【从网络访问此计算机 属性】对话框。文本框中显示了允许通过网络访问该计算机的用户或组(图 9-29)。如果要删除一些用户或组(禁止他们通过网络访问该计算机)，可以先选择要删除的用户或组，然后单击【删除】按钮即可。如果需要添加一些用户或组通过网络访问该计算机，则单击【添加用户或组】按钮，然后按提示操作即可。

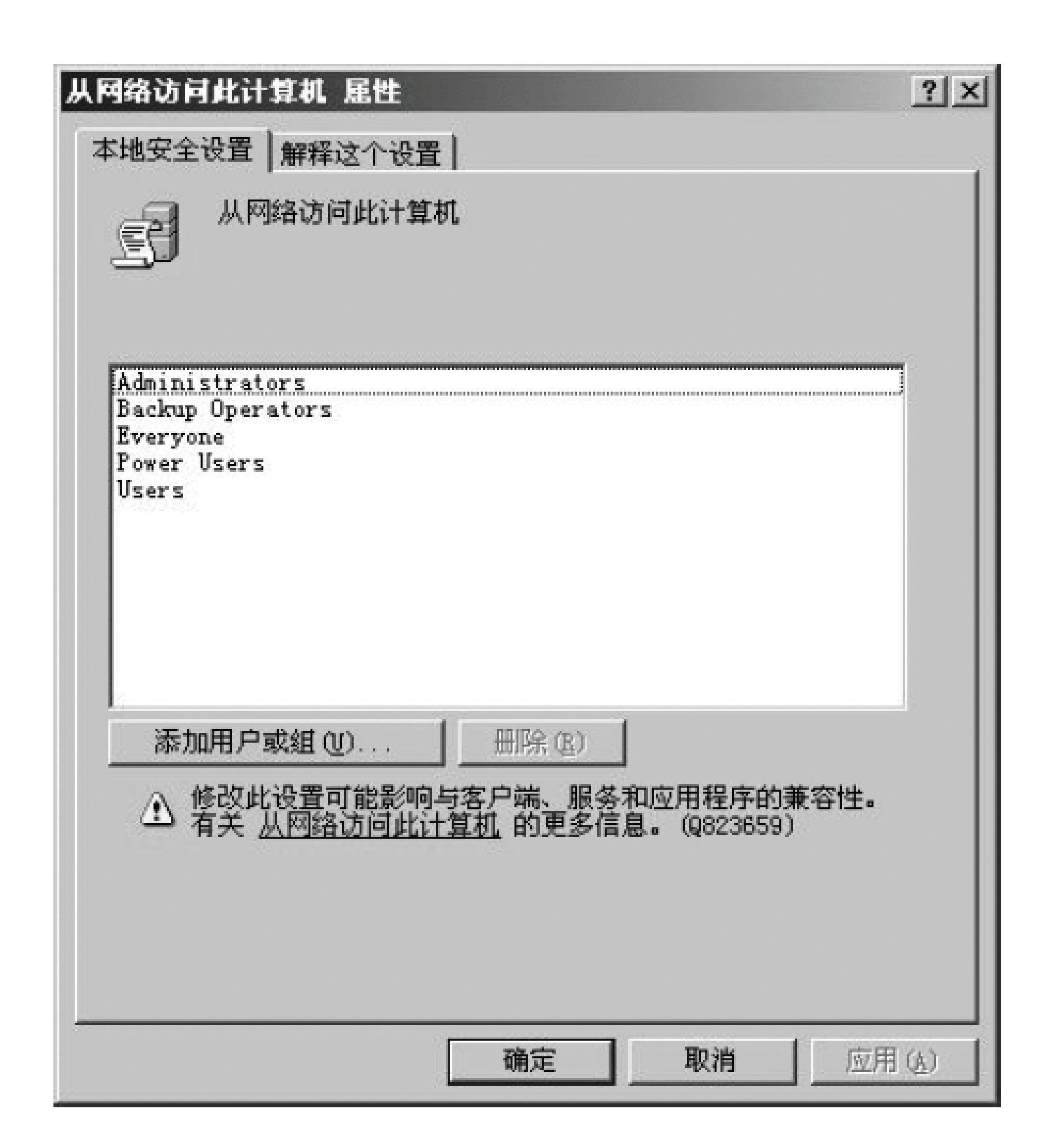


图 9-29　【从网络访问此计算机 属性】对话框

有关该权限的详细解释可以通过选择【解释这个设置】选项卡查看。

(2) 从远程系统强制关机。该安全设置确定允许哪些用户从网络上的远程位置关闭计算机。误用此用户权限会导致拒绝服务。设置方法参考(1)。

(3) 管理审核和安全日志。该安全设置确定哪些用户可以为单独的资源(如文件、Active Directory 对象和注册表项)指定对象访问审核选项。设置方法参考(1)。

(4) 允许在本地登录。该登录权限确定哪些用户能以交互方式登录到该计算机。设置方法参考(1)。

3. 安全选项

安全选项用于控制一些与操作系统安全相关的设置，包括设置网络服务器、网络用户、关机、交互式登录、设备、审计、网络安全、网络访问、系统加密、域控制器、账户等约 64 个策略选项。

在图 9-21 所示的左侧窗口的目录树中，选择【本地策略】/【安全选项】选项，打开如图 9-30



所示的【安全选项】属性窗口。在右侧详细信息列表窗格中显示可配置的安全选项的当前配置。



图 9-30 【安全选项】属性窗口

下面只对几个常用的策略选项作介绍，其他策略选项可以根据需要参考下列的方法进行设置。

(1) 关机：允许在未登录前关机。在如图 9-30 所示的右侧详细信息列表窗格中，双击【关机：允许系统在未登录前关机】选项，打开【关机：允许系统在未登录前关机 属性】对话框(图 9-31)。在默认选择的【本地安全设置】选项卡中，通过选择【已启用】或【已禁用】单选按钮，启用或禁用该策略。

(2) 交互式登录：用户试图登录时消息标题。在如图 9-30 所示的右侧详细信息列表窗格中，双击【交互式登录：用户试图登录时消息标题】选项，打开如图 9-32 所示的对话框。在默认打开的【本地安全设置】选项卡的文本框中，可以输入用户登录时出现的消息文本窗口的标题栏中显示的标题说明。默认设置为无消息。

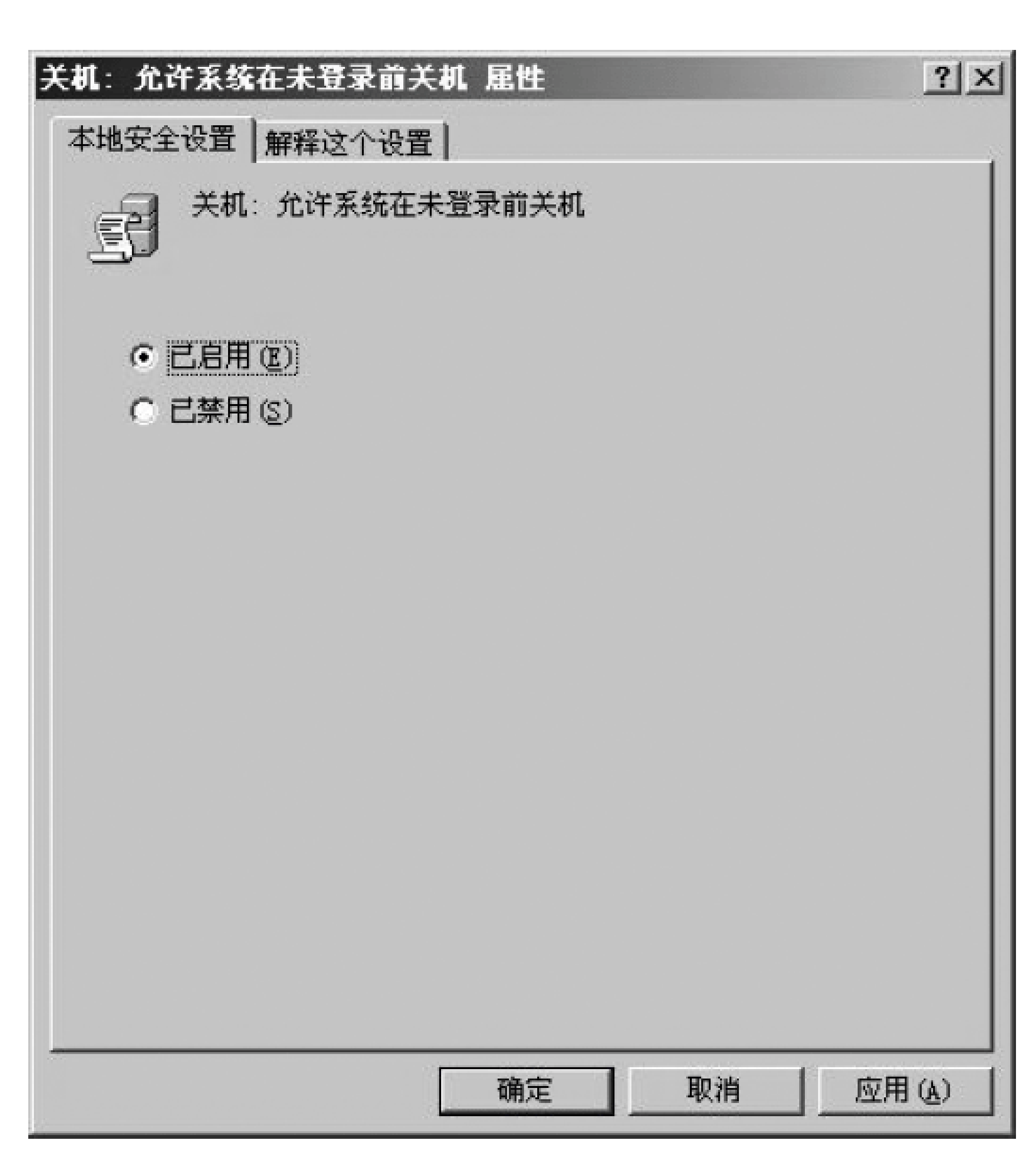


图 9-31 【关机：允许系统在未登录前关机 属性】对话框



图 9-32 【交互式登录：用户试图登录时消息标题 属性】对话框



（3）交互式登录：用户试图登录时消息文字。在如图 9-30 所示的右侧详细信息列表窗格中，双击【交互式登录：用户试图登录时消息文字】选项，打开如图 9-33 所示的对话框。在默认打开的【本地安全设置】选项卡的文本框中，可以输入用户登录时出现的消息文本窗口中显示的文本消息。默认设置为无消息。

（4）交互式登录：在密码到期前提示用户更改密码。在如图 9-30 所示的右侧详细信息列表窗格中，双击【交互式登录：在密码到期前提示用户更改密码】选项，打开如图 9-34 所示的对话框。在默认打开的【本地安全设置】选项卡中可以设置提前多少天向用户发出其密码过期的警告。默认值为 14 天。

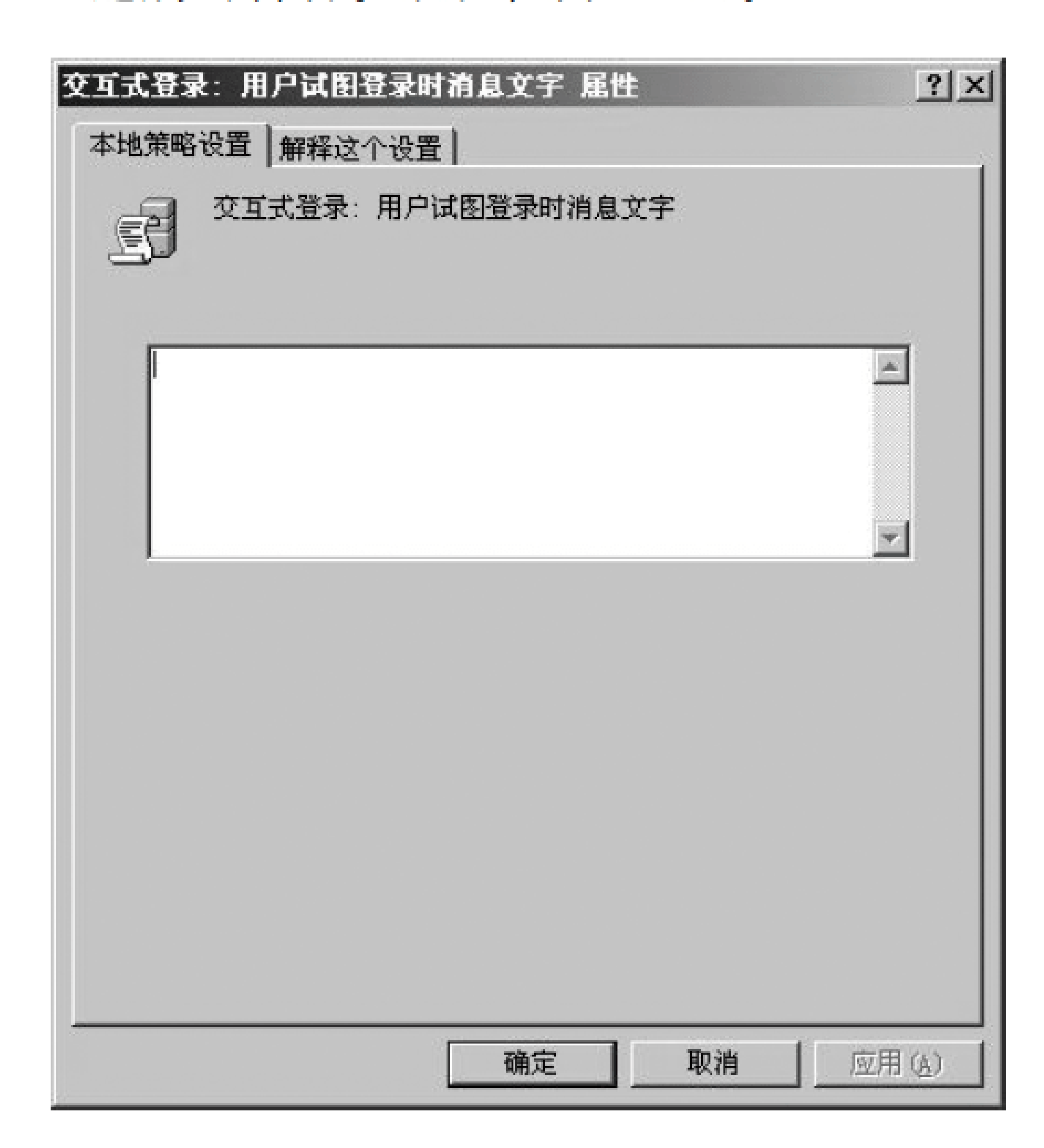


图 9-33　【交互式登录：用户试图登录时消息文字 属性】对话框



图 9-34　【交互式登录：在密码到期前提示用户更改密码 属性】对话框

9.5　本地安全策略的应用

为了更好地说明本地安全策略的作用，下面分别介绍账户策略设置、用户权限分配设置和安全选项设置的应用。

9.5.1　账户策略设置

本地安全策略的账户策略设置在独立的计算机上进行设置，如果要设置账户的密码长度最小为 10，账户如果连续 3 次输错密码就会被锁定。步骤如下：

（1）以 Administrator 账户登录系统（建议采用 Windows Server 2003 R2 EnterPrise Edition），选择【开始】/【程序】/【管理工具】/【本地安全策略】命令，打开【本地安全设置】窗口（图 9-21），在左侧窗口的目录树中，选择【账户策略】/【密码策略】选项，打开如图 9-22 所示的【密码策略】属性窗口。



(2) 在右侧详细信息列表窗格中双击【密码长度最小值】选项,打开【密码长度最小值属性】对话框,在文本框中输入 10(图 9-35)。单击【确定】按钮。

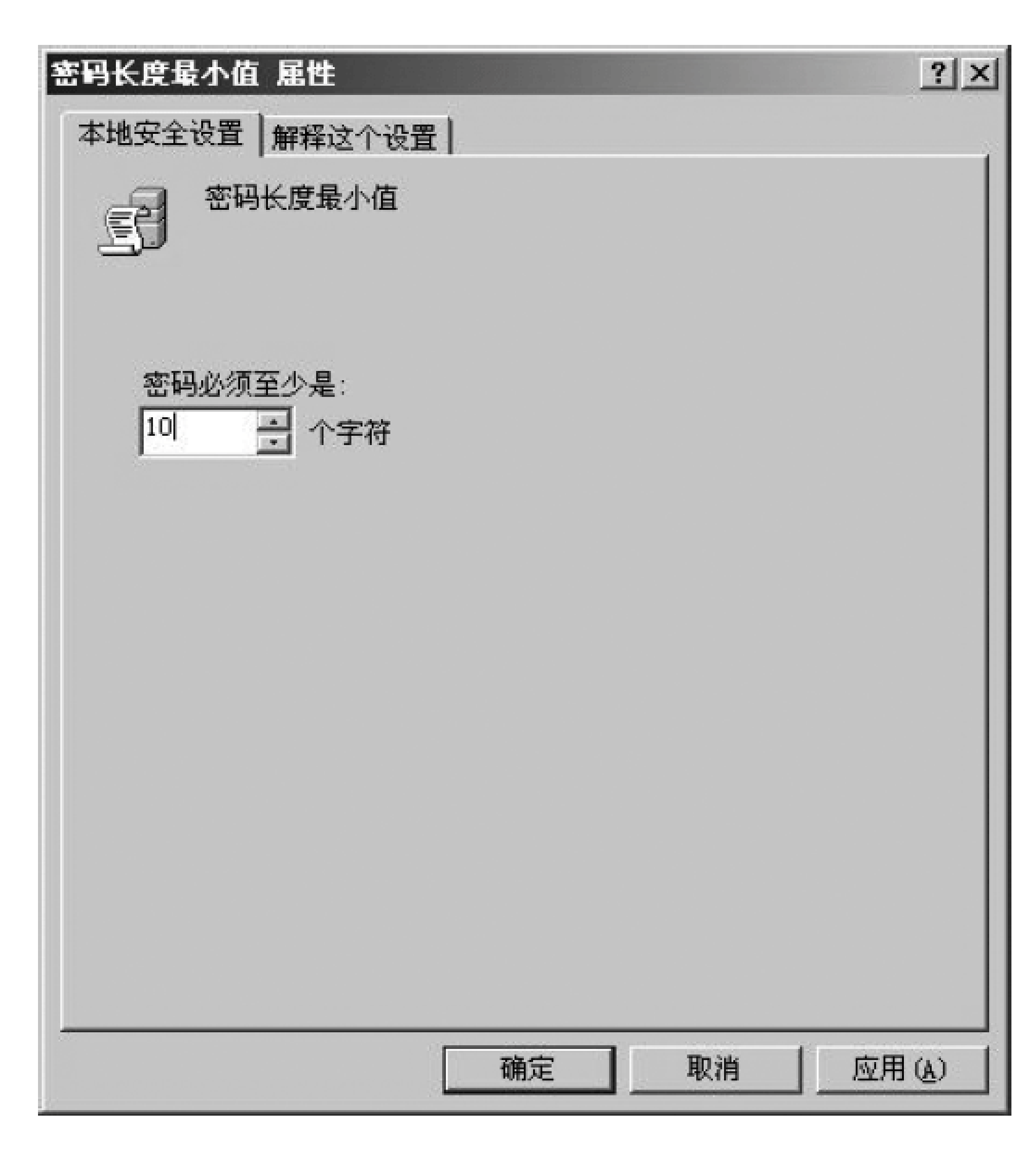


图 9-35 【密码长度最小值 属性】对话框

(3) 在左侧窗口的目录树中选择【账户锁定策略】选项,在右侧详细信息列表窗格中双击【账户锁定阈值】选项,打开【账户锁定阈值 属性】对话框,在文本框中输入 3。单击【确定】按钮后,会弹出【建议的数值改动】对话框(图 9-36),单击【确定】按钮即可完成。

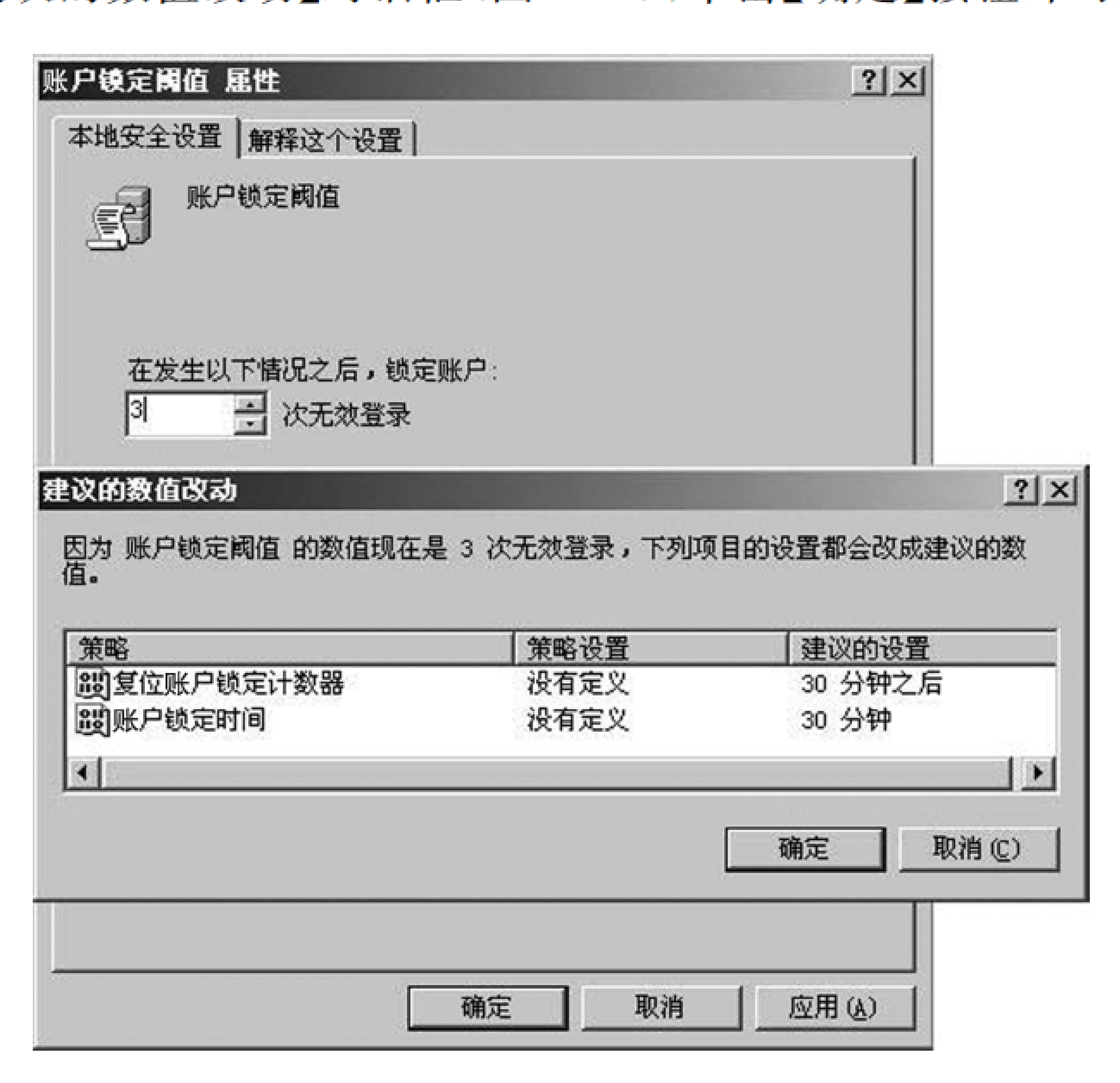


图 9-36 【账户锁定阈值 属性】对话框

(4) 选择【开始】/【运行】命令,在打开的【运行】对话框中输入 gpupdate 命令(图 9-37),



单击【确定】按钮，刷新本计算机的本地安全策略（或者重启计算机）。

注意：计算机策略（包括此处介绍的本地安全策略，以及后面将要介绍的域控制器安全策略、域安全策略和组策略）修改之后，必须使用 gpupdate 命令进行刷新或重启，修改后的策略才会生效。

（5）验证。创建一个用户账户（如 offi001），设置长度小于 10 的密码，结果弹出错误信息提示对话框（图 9-38）。设置长度大于等于 10 的密码，创建成功。



图 9-37　【运行】对话框

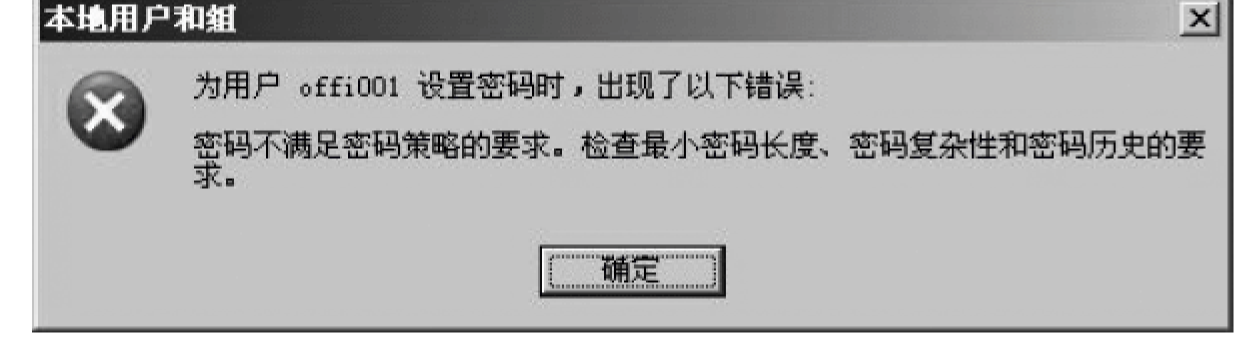


图 9-38　错误信息提示对话框

（6）退出系统，以普通账户 offi001 登录，故意输错密码 3 次，结果该账户被锁定（图 9-39）。



图 9-39　账户被锁定提示对话框

（7）以 Administrator 账户登录系统，打开如图 9-40 所示的【offi001 属性】对话框，可以看到【账户已锁定】复选框被自动选中了，说明该账户处于被锁定状态。取消对【账户已锁定】复选框的选择，单击【确定】按钮，即可解除对该账户的锁定。

（8）验证。退出系统，再次以 offi001 账户登录，能成功登录则说明设置正确。



图 9-40　【offi001 属性】对话框

9.5.2　用户权限分配设置

如果想通过设置不允许普通用户在本地登录，则需要在用户权限分配中进行设置。设置步骤如下：

（1）以 Administrator 账户登录系统（建议采用 Windows Server 2003 R2 EnterPrise Edition），选择【开始】/【程序】/【管理工具】/【本地安全策略】命令，打开【本地安全设置】窗口（图 9-21），在左侧窗口的目录树中，选择【本地策略】/【用户权限分配】选项，打开如图 9-28 所示的【用户权限分配】属性窗口。



（2）在右侧详细信息列表窗格中双击【允许在本地登录】选项，默认打开【本地安全设置】选项卡，选择【允许在本地登录】文本框中的 Power Users 和 Users 选项（图 9-41）。单击【删除】按钮，可以看到这两个普通用户组已从允许本地登录的成员列表中删除（图 9-42）。

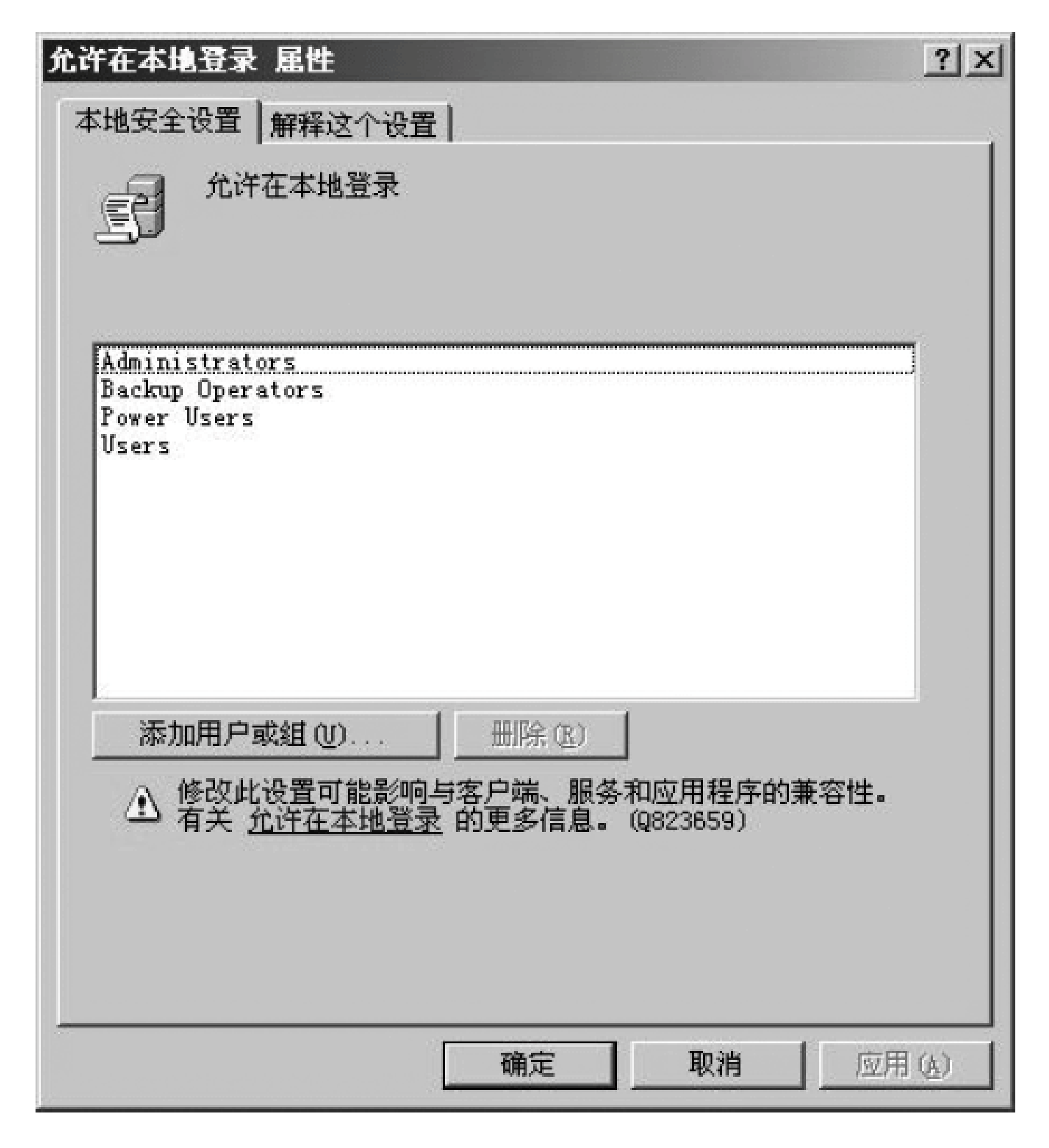


图 9-41 【允许在本地登录 属性】对话框（一）

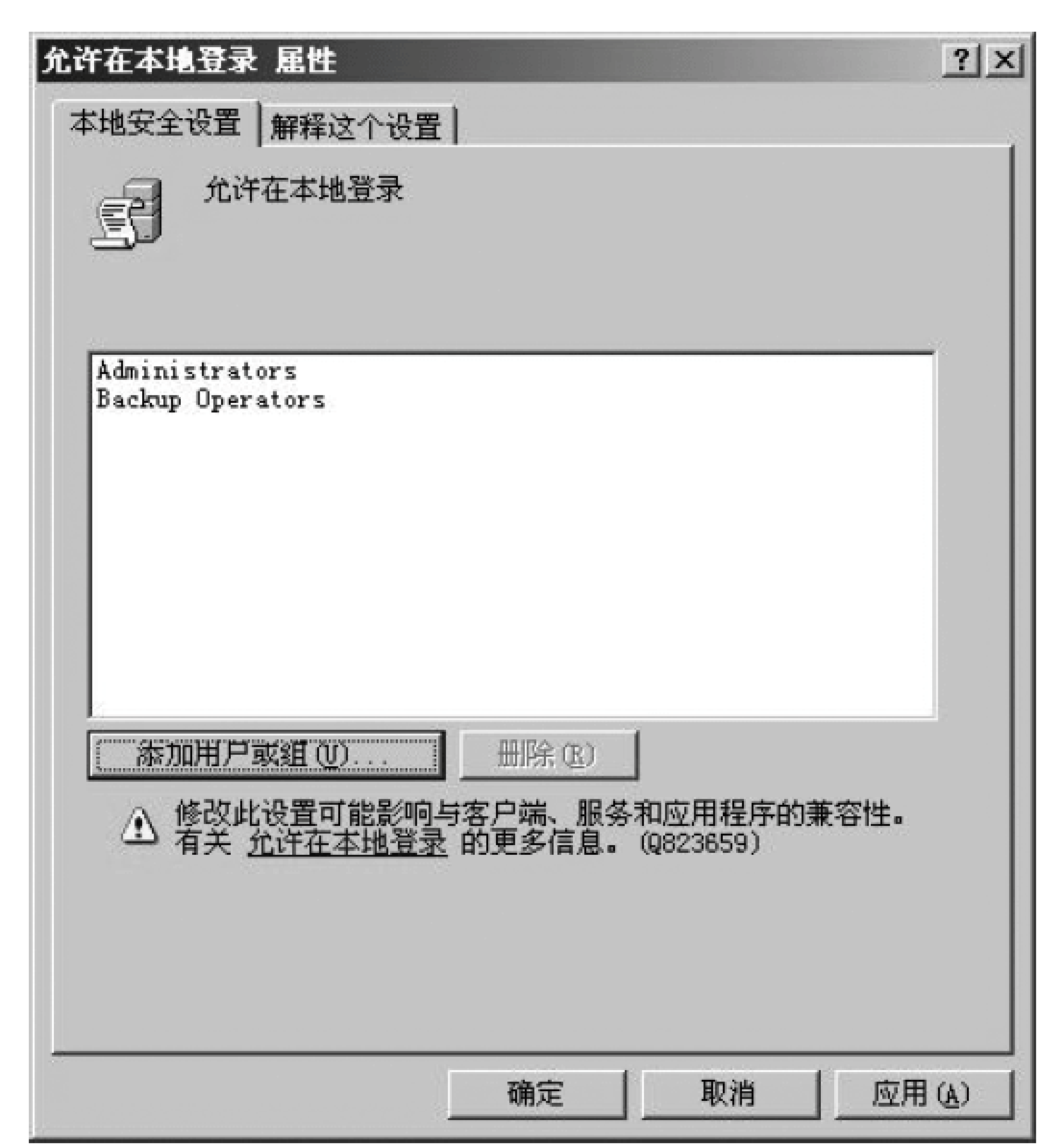


图 9-42 【允许在本地登录 属性】对话框（二）

（3）单击【确定】按钮，确认所作的更改。

（4）选择【开始】/【运行】命令，在打开的【运行】对话框中输入 gpupdate 命令，刷新本计算机的本地安全策略（或者重启计算机）。

（5）验证。退出系统，使用普通用户账户 offi001 登录，出现不允许交互登录的提示（图 9-43），说明设置成功。



图 9-43 不允许登录提示对话框

9.5.3 安全选项设置

如果想让用户在登录系统前必须阅读使用该计算机的注意事项，那么就需要在安全选项中进行相关设置。步骤如下：

（1）以 Administrator 账户登录系统（建议采用 Windows Server 2003 R2 EnterPrise Edition），选择【开始】/【程序】/【管理工具】/【本地安全策略】命令，打开【本地安全设置】窗口（图 9-21），在左侧窗口的目录树中，选择【本地策略】/【安全选项】选项，打开如图 9-30 所示的【安全选项】属性窗口。

（2）在右侧详细信息列表窗格中双击【交互式登录：用户试图登录时消息标题】选项，打开如图 9-32 所示的对话框。在默认打开的【本地安全设置】选项卡的文本框中输入“请您注意”。然后单击【确定】按钮，返回【安全选项】属性窗口。

（3）在右侧详细信息列表窗格中双击【交互式登录：用户试图登录时消息文字】选项，



打开如图 9-33 所示的对话框。在默认打开的【本地安全设置】选项卡的文本框中输入“未经许可，不能使用外来储存设备”。然后单击【确定】按钮。

（4）选择【开始】/【运行】命令，在打开的【运行】对话框中输入 gpupdate 命令，刷新本计算机的本地安全策略。

（5）验证。注销账户，重新登录。在按下 Ctrl＋Alt＋Del 组合键后，弹出如图 9-44 所示的【请您注意】（第（2）步中设置的标题）对话框，文本框中的内容就是第（3）步设置的内容。单击【确定】按钮后，才进入登录对话框。



图 9-44　用户登录前弹出的消息提示对话框

9.6　域控制器安全策略

9.6.1　域控制器安全策略简介

将一台服务器安装了 AD 后，就升级为域控制器，在域控制器中，本地安全策略被域控制器安全策略代替。因此，域控制器安全策略与本地安全策略的选项及其用法大部分是相同的，不再赘述。下面仅对两者的不同之处进行说明。

1. 域控制器安全策略与本地安全策略的区别

（1）影响的计算机不同。域控制器安全策略影响的是域控制器，而本地安全策略影响的是非域控制器。

（2）打开的方式不同。域控制器安全策略的打开方式为：选择【开始】/【程序】/【管理工具】/【域控制器安全策略】命令。

本地安全策略的打开方式为：选择【开始】/【程序】/【管理工具】/【本地安全策略】命令。

（3）账户策略有区别。域控制器安全策略的账户策略与域用户账户的登录有关，且增加了 Kerberos 策略。而本地安全策略的账户策略与本地用户账户的登录有关。

下面详细介绍 Kerberos 策略。

注意：对于两种安全策略共同拥有的策略选项，在域控制器安全策略中的用法和默认设置可能会有所不同，这些不同之处在上面介绍本地安全策略时已经作了说明。

2. Kerberos 策略

Kerberos 是一种网络认证协议，其设计目标是通过密钥系统为客户机/服务器应用程序提供强大的认证服务。该认证过程的实现不依赖于主机操作系统的认证，无须基于主机地址的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意地



读取、修改和插入数据。在上述情况下，Kerberos 作为一种可信任的第三方认证服务，通过传统的密码技术（如共享密钥）执行认证服务。Kerberos V5（即 Kerberos 版本 5）是面向 Windows Server 2003 中的服务和应用程序的默认网络身份验证方法。

Kerberos 策略用于域用户账户，用于确定与 Kerberos 相关的设置，包括服务票证最长寿命、计算机时钟同步的最大容差、强制用户登录限制、用户票证续订最长寿命、用户票证最长寿命等。

注意：票证是 Kerberos 身份验证的基本单位。它是严谨构造的、在计算机之间传递的消息，其中包括身份验证信息。

Windows 中的两种票证形式是票证授予式票证（Ticket-Granting Ticket，TGT）和服务票证。TGT 是用户登录时，KDC 颁发给用户的凭据。当服务要求会话票证时，用户必须向 KDC 递交 TGT，因为 TGT 对于用户的登录会话活动通常是有效的，它有时称为"用户票证"。

服务票证是由允许用户验证域中指定服务的 Kerberos V5 票证授予服务（Ticket-Granting Service，TGS）颁发的票证。如果客户端请求服务器连接时出示的会话票证已过期，服务器将返回错误消息。客户端必须从 KDC 请求新的会话票证。然而一旦连接通过了身份验证，该会话票证是否仍然有效就无关紧要了。会话票证仅用于验证和服务器的新建连接。

选择【开始】/【程序】/【管理工具】/【域控制器安全策略】命令，打开【默认域控制器安全设置】对话框，在左侧窗口的目录树中，选择【Windows 设置】/【安全设置】/【账户策略】/【Kerberos 策略】选项，打开【Kerberos 策略】属性窗口（图 9-45），在右侧详细信息列表窗格中显示了可配置的 Kerberos 策略的当前配置。下面详细介绍如下。

（1）强制用户登录限制。该策略确定 Kerberos V5 密钥分发中心（Kerberos Key Distribution Center，KDC）是否要根据用户账户的用户权限来验证每一个会话票证请求。验证每一个会话票证请求是可选的，因为额外的步骤需要花费时间，并可能降低服务的网络访问速度。默认值为启用。

（2）服务票证最长寿命。该策略确定使用所授予的会话票证可访问特定服务的最长时间（以分钟为单位）。该设置必须大于 10 分钟并且小于或等于下面将要介绍的"用户票证最长寿命"设置。默认值为 600 分钟。

双击图 9-45 右侧详细信息列表窗格中的【服务票证最长寿命】选项，打开【服务票证最长寿命 属性】对话框，选中【定义这个策略设置】复选框后，可以在【票证过期时间】下的文本框中输入时间值。单击【确定】按钮后，会弹出【建议的数值改动】对话框（图 9-46），单击【确定】按钮即可完成。

（3）用户票证最长寿命。该策略确定用户 TGT 的最长使用时间（单位为小时）。用户 TGT 期满后，必须请求新的或"续订"现有的用户票证。默认值为 10 小时。

（4）用户票证续订最长寿命。该策略确定可以续订用户 TGT 的期限（以天为单位）。默认值为 7 天。

（5）计算机时钟同步的最大容差。该策略确定 Kerberos V5 所允许的客户端时钟和提供 Kerberos 身份验证的 Windows Server 2003 域控制器上的时间的最大差值（以分钟为单

位）。默认值为 5 分钟。



图 9-45　【Kerberos 策略】属性窗口



图 9-46　【服务票证最长寿命 属性】对话框

注意：为防止“轮番攻击”，Kerberos V5 在其协议定义中使用了时间戳。为使时间戳正常工作，客户端和域控制器的时钟应尽可能保持同步。换言之，应该将这两台计算机设置成相同的时间和日期。因为两台计算机的时钟常常不同步，所以管理员可使用该策略来设置 Kerberos V5 所能接受的客户端时钟和域控制器时钟间的最大差值。如果客户端时钟和域控制器时钟间的差值小于该策略中指定的最大时间差，那么在这两台计算机的会话中使用的任何时间戳都将被认为是可信的。该设置并不是永久性的。如果配置该设置后重新启动计算机，那么该设置将被还原为默认值。



9.6.2 域控制器安全策略设置应用

如果需要允许域中 info 组所有用户账户可以在 DC 上登录，设置步骤如下：

(1) 以 Administrator 账户登录域控制器，选择【开始】/【程序】/【管理工具】/【域控制器安全策略】命令，打开【默认域控制器安全设置】对话框，在左侧窗口的目录树中，选择【安全设置】/【本地策略】/【用户权限分配】选项，打开【用户权限分配】属性窗口(图 9-47)。



图 9-47 【用户权限分配】属性窗口

(2) 在右侧详细信息列表窗格中双击【允许在本地登录】选项，打开【允许在本地登录属性】对话框(图 9-48)，图中文本框显示了允许在本地登录的用户或组。

(3) 单击【添加用户或组】按钮，打开【选择用户或组】对话框。单击【浏览】按钮，打开【选择用户、计算机或组】对话框(图 9-49)。

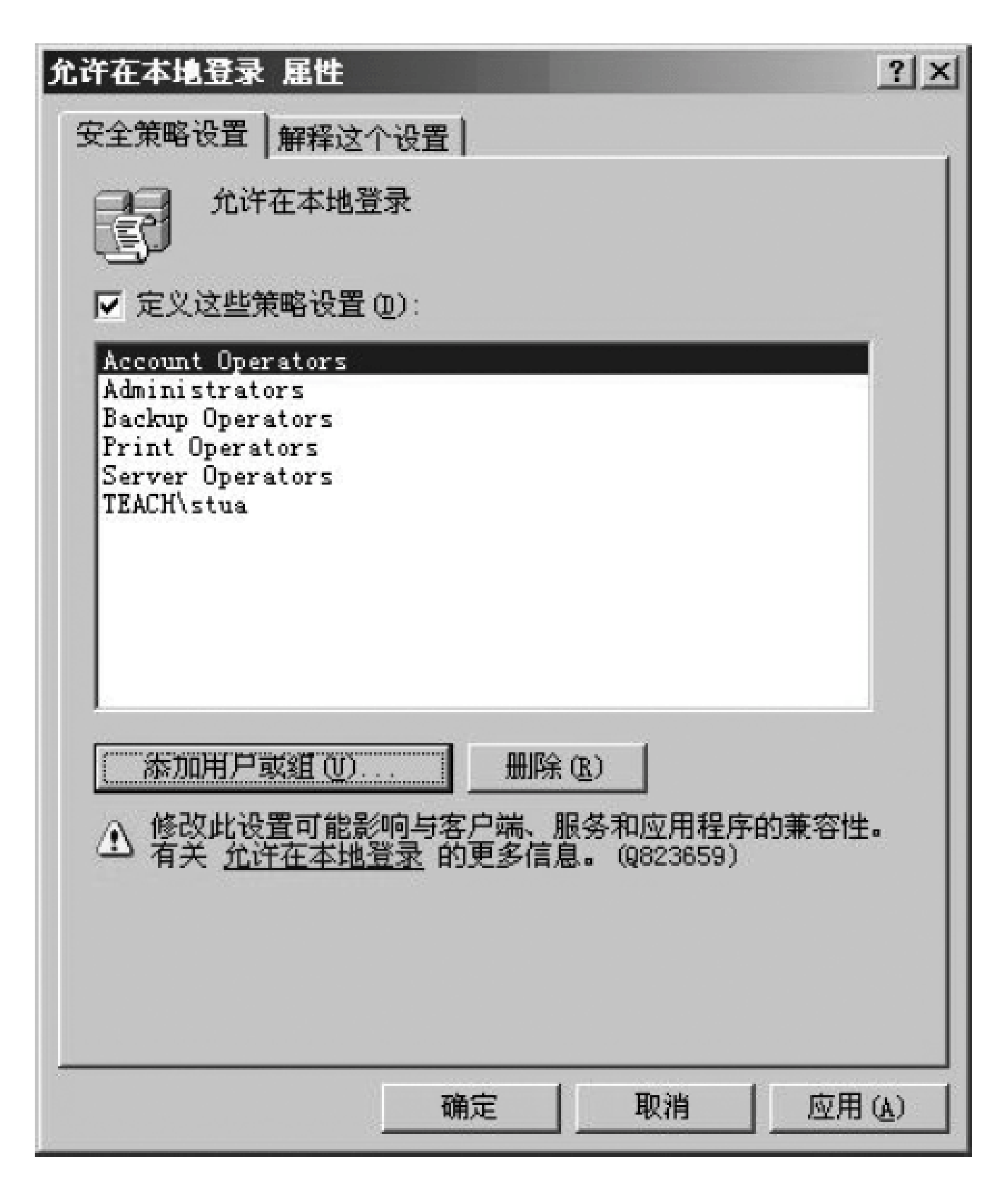


图 9-48 【允许在本地登录 属性】对话框

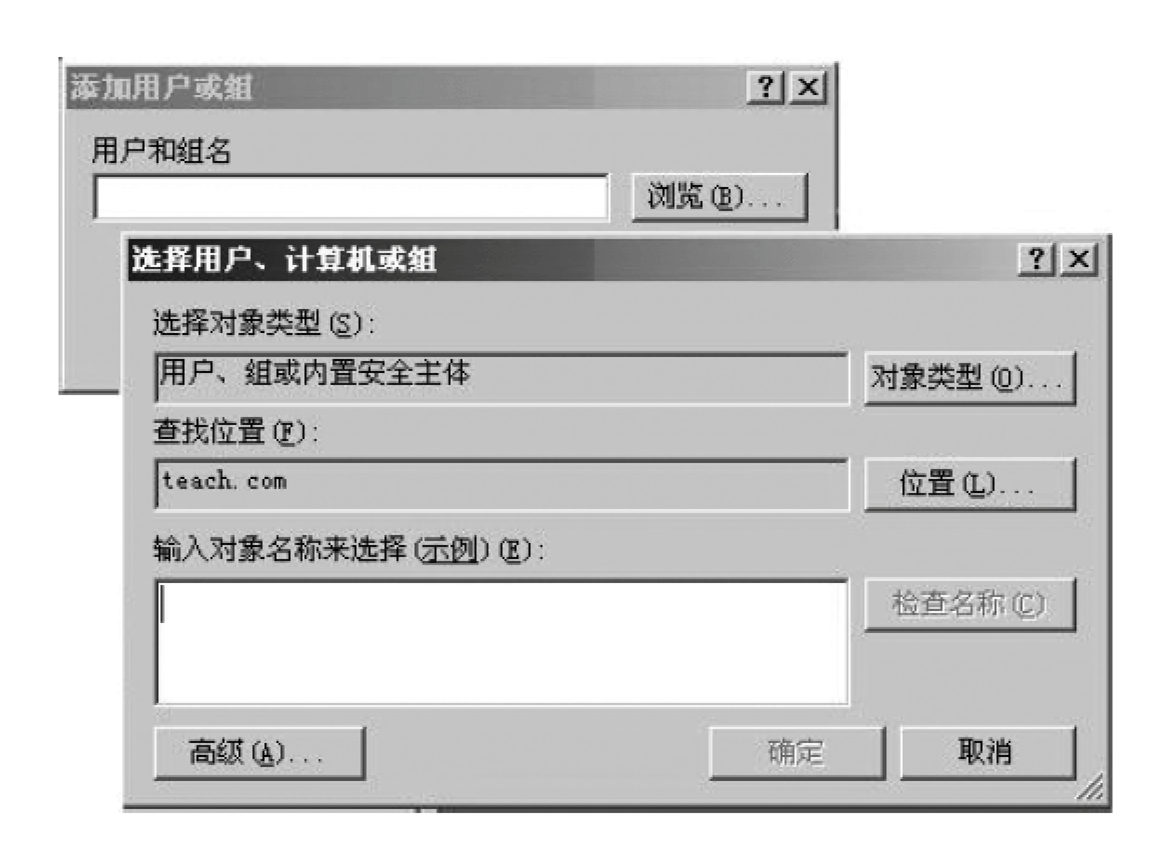


图 9-49 【选择用户、计算机或组】对话框





(4) 单击【高级】按钮,打开【选择用户、计算机或组】高级对话框。单击【立即查找】按钮,在【搜索结果】文本框中会显示域中所有成员,利用滚动条找到并选择 info 组(图 9-50)。



图 9-50　在【搜索结果】文本框中选择 info 组

(5) 单击【确定】按钮。依次返回上一级对话框,依次单击【确定】按钮,直到关闭所有对话框。设置完成。

(6) 选择【开始】/【运行】命令,在打开的【运行】对话框中输入 gpupdate 命令,刷新本计算机的本地安全策略。

(7) 验证。注销 Administrator,以 info 组中的用户账户 info001 登录域控制器,能成功登录则说明设置正确。

9.7　域安全策略

当一台服务器通过安装 AD 升级为域控制器后,域控制器安全策略代替了本地安全策略,同时还增加了对整个域进行安全保护的域安全策略。

域安全策略的打开方式为:选择【开始】/【程序】/【管理工具】/【域安全策略】命令(图 9-51),可以看到其选项与域控制器安全策略选项完全相同,那么,本地安全策略、域控制器安全策略和域安全策略三者之间有什么联系和区别呢?当这些策略设置项作用于同一台计算机上发生冲突时,哪一种策略优先呢?

下面,首先介绍这三种安全策略之间的关系,然后介绍域安全策略中几个重要策略的应用。





图 9-51 【默认域安全设置】窗口

9.7.1 三种安全策略的关系

1. 三种安全策略的作用范围不同

(1) 本地安全策略是本地策略的一部分,在计算机启动后就会被执行,无论该计算机是处于工作组模式还是域模式。

(2) 域安全策略是域策略的一部分,它影响整个域中的所有计算机,因此一台计算机只要处于域模式,就会采用域策略。

(3) 域控制器安全策略是 OU 策略的一种,它的作用范围是域控制器。

它们之间的关系可以用图 9-52 表示。

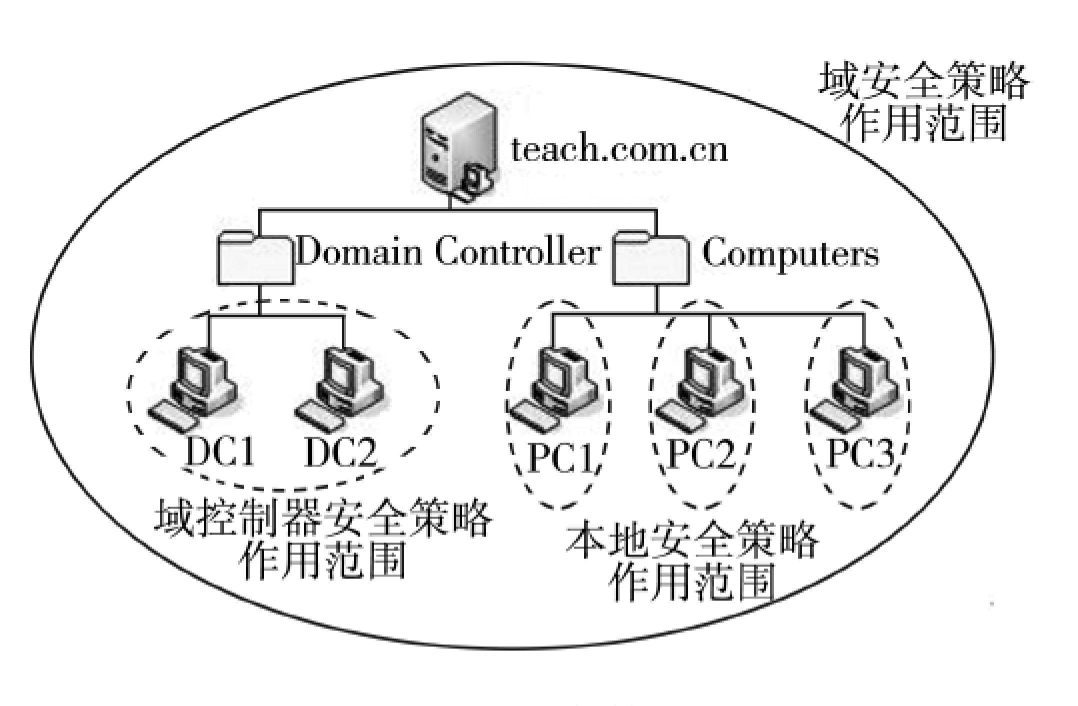


图 9-52 三种安全策略的关系

2. 三种安全策略的优先级

除了账户策略以外,当客户端的本地安全策略与域安全策略的设置项发生冲突时,域安全策略优先;当域控制器安全策略与域安全策略的设置项发生冲突时,域控制器安全策略优先。对于账户策略,域安全策略优先级最高。

> **注意:** 当同一种安全策略中的允许策略与拒绝策略冲突时,拒绝策略优先于允许策略。但是,如果允许策略与拒绝策略分别在不同种类的安全策略中设置,则遵循上述优先级规则。

3. 优先级验证

通过下列的设置验证三种安全策略的优先级。

(1) 本地安全策略与域安全策略的设置项冲突(表 9-6),设置及验证步骤如下:



表 9-6　本地安全策略与域安全策略的设置项设置情况

设　置　项	本地安全策略	域安全策略
密码长度最小值	第 1 次：设为 3 第 2 次：设为 8	第 1 次：设为 8 第 2 次：设为 3

① 在域中一台安装了 Windows 2000/XP 的客户端上，以 Administrator 账户登录，设置本地安全策略：密码长度最小值(设为 3)。详细操作步骤参考 9.5.1 小节。

② 在域控制器中，以 Administrator 账户登录，设置域安全策略：密码长度最小值(设为 8)。

③ 在客户端上修改用户账户 offic001 的密码，设置长度大于等于 3 且小于 8 的密码，结果弹出如图 9-38 所示错误信息提示对话框。

④ 试将本地安全策略的密码长度最小值设置为 8，而域安全策略的密码长度最小值设置为 3，修改用户账户 offic001 的密码为长度大于等于 3 且小于 8 的值。结果修改成功。

上述实例验证了当客户端的本地安全策略与域安全策略的设置项发生冲突时，域安全策略优先。

(2) 域控制器策略与域安全策略的设置项冲突(表 9-7)，设置及验证步骤如下：

表 9-7　域控制器安全策略与域安全策略的设置项设置情况

设　置　项	域控制器安全策略	域安全策略
交互式登录：用户试图登录时消息标题	请您注意	欢迎您
交互式登录：用户试图登录时消息文字	未经许可，不能使用外来储存设备!	欢迎您来到××公司!

① 以 Administrator 账户登录域控制器，设置域控制器安全策略的“交互式登录：用户试图登录时消息标题”选项为“请您注意”；设置“交互式登录：用户试图登录时消息文字”选项为“未经许可，不能使用外来储存设备!”(详细操作步骤参考 9.6.2 小节)。

② 设置域安全策略的“交互式登录：用户试图登录时消息标题”选项为“欢迎您”；设置“交互式登录：用户试图登录时消息文字”选项为“欢迎您来到××公司!”。

③ 运行 gpupdate 命令，刷新安全策略。

④ 注销账户，重新登录，结果弹出如图 9-44 所示的【请您注意】对话框。

上述实例验证了当域控制器策略与域安全策略的设置项冲突时，域控制器安全策略优先。

(3) 允许策略与拒绝策略冲突(表 9-8)，设置及验证步骤如下。

表 9-8　域控制器安全策略与域安全策略的设置项设置情况-1

设　置　项	域控制器安全策略	域安全策略
允许在本地登录	第 1 次：默认(无允许 other001) 第 2 次：添加 other001	允许 other001
拒绝本地登录	默认(无拒绝 other001)	拒绝 other001

① 以 Administrator 账户登录域控制器，设置域安全策略的“允许在本地登录”选项，添加用户账户 other001；设置“拒绝在本地登录”选项，添加用户账户 other001(详细操作步骤



参考 9.6.2 小节)。

② 检查域控制器安全策略的“允许本地登录”选项,确认无用户账户 other001;检查“拒绝本地登录”选项,确认无用户账户 other001。

③ 运行 gpupdate 命令,刷新安全策略。

④ 注销 Administrator 账户,以 other001 账户登录,结果弹出如图 9-43 所示不允许交互登录的提示。

⑤ 重新以 Administrator 账户登录,修改域控制器安全策略的“允许在本地登录”选项,添加用户账户 other001。

⑥ 运行 gpupdate 命令,刷新安全策略。

⑦ 注销 Administrator 账户,以 other001 账户登录,结果能正常登录。

上述实例验证了当同一种安全策略中的允许策略与拒绝策略冲突时,拒绝策略优先于允许策略;但是,如果允许策略与拒绝策略分别在不同种类的安全策略中设置,则遵循上述优先级规则。

(4) 域控制器的账户策略与域的账户策略的设置项冲突(表 9-9),设置及验证步骤如下:

表 9-9 域控制器安全策略与域安全策略的设置项设置情况

设　置　项	域控制器安全策略	域安全策略
密码长度最小值	第 1 次:设为 3 第 2 次:设为 8	第 1 次:设为 8 第 2 次:设为 3

① 以 Administrator 账户登录域控制器,设置域控制器安全策略:密码长度最小值(设为 3)。详细操作步骤参考 9.5.1 小节。

② 设置域安全策略:密码长度最小值(设为 8)。

③ 修改用户账户 offic001 的密码,设置长度大于等于 3 且小于 8 的密码,结果弹出如图 9-38所示的错误信息提示对话框。

④ 试将域控制器安全策略的密码长度最小值设置为 8,而域安全策略的密码长度最小值设置为 3,再次修改用户账户 offic001 的密码为长度大于等于 3 且小于 8 的值。结果修改成功。

上述设置验证了对于账户策略,域安全策略优先级最高。

9.7.2 审核文件及文件夹

作为域管理员,为了保障整个域的安全性,必须设置相应的策略以便能及时发现威胁,并采取应对措施,将威胁消灭在萌芽状态。因此,在域安全策略中创建一个有效的审核策略是很重要的,以定义需要报告的安全事件。例如,某用户账户多次登录失败、某用户账户频繁尝试访问其他账户加密的文件、某用户账户试图对审核策略进行更改等。

但是,如果审核策略设置的审核事件过多,导致许多授权活动都生成事件,则安全日志将被大量无用的数据占满,最早的审核项将被覆盖。因此,审核策略必须根据实际环境和用户的要求来设置。



1. 审核策略设置建议

在一般情况下，审核策略选项的设置建议如下（审核策略的一般用法可以参考 9.4.2 小节）。

- 审核账户登录事件：成功、失败

该策略审核域用户账户从域中的计算机登录时，域控制器收到的验证信息。如果仅审核成功的操作，则未经授权的入侵尝试将不会出现在日志中。未经授权的入侵尝试的特征是出现大量的不成功操作。

- 审核账户管理：成功、失败

该策略审核计算机上的每一个用户账户管理事件，包括创建、更改或删除用户账户或组；重命名、禁用或启用用户账户；设置或更改密码。

- 审核目录服务访问：失败

该策略审核用户访问活动目录对象的事件。

- 审核登录事件：成功、失败

该策略审核所有计算机用户的登录和注销事件。

- 审核对象访问：失败

该策略审核用户访问某个对象的事件，例如文件、文件夹、注册表项、打印机等。

- 审核策略更改：成功、失败

该策略审核对用户权限分配策略、审核策略更改的每一个事件。

- 审核特权使用：失败

该策略审核用户实施其用户权利的每一个事件。

- 审核过程跟踪：无审核

该策略审核对事件的详细跟踪信息。如果设置为“失败”，则审核事件跟踪用户对无权访问区域的访问尝试。

- 审核系统事件：成功、失败

该策略审核用户重新启动或关闭计算机时或者对系统安全或安全日志有影响的事件。

2. 审核文件及文件夹

在此以对文件或文件夹设置审核策略为例，说明审核策略的用法及其设置步骤。

（1）启用域或者本机的审核策略中的审核对象访问策略，并刷新策略。

在如图 9-51 所示的【审核策略】属性窗口的右侧详细信息列表窗格中双击【审核对象访问】选项，打开【审核对象访问 属性】对话框，选中【定义这些策略设置】复选框，选中【失败】复选框（图 9-53）。单击【确定】按钮。运行 gpupdate 命令，刷新安全策略。

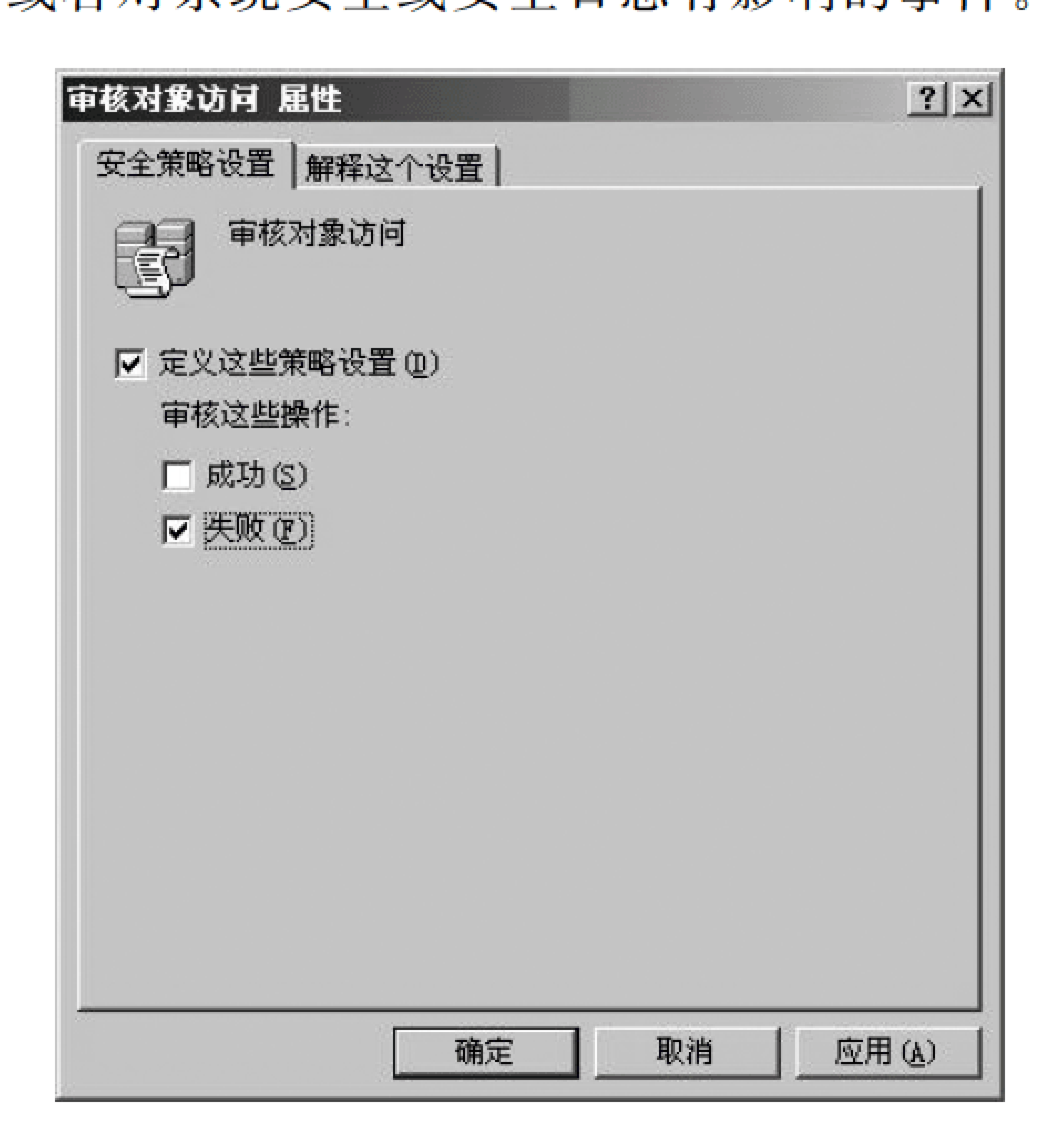


图 9-53 【审核对象访问 属性】对话框

（2）在需要审核的文件或文件夹的【高级安全设置】/【审核】中，添加要审核的账户及详



细的审核项目。

例如，在需要审核的文件 Eula. txt 上右击，在弹出的【Eula. txt 属性】对话框中选择【安全】选项卡，单击【高级】按钮，打开【Eula. txt 的高级安全设置】对话框。选择【审核】选项卡（图 9-54），单击【添加】按钮，参考 9. 6. 2 小节的步骤，添加要审核的账户（如 stu001）。依次单击【确定】按钮后打开【Eula. txt 的审核项目】对话框（图 9-55），在此可设置详细的审核项目。

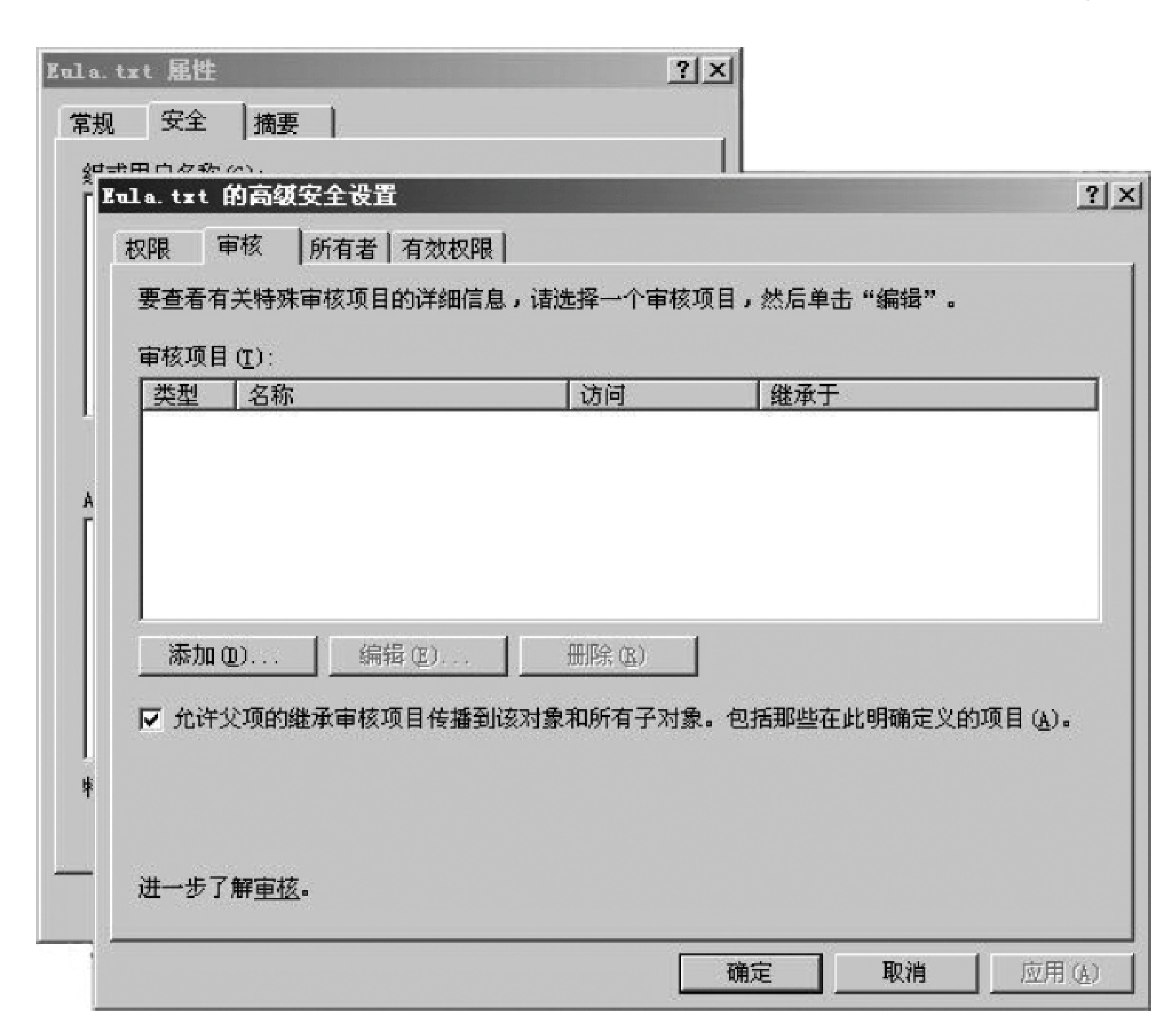


图 9-54 【Eula. txt 的高级安全设置】对话框的【审核】选项卡

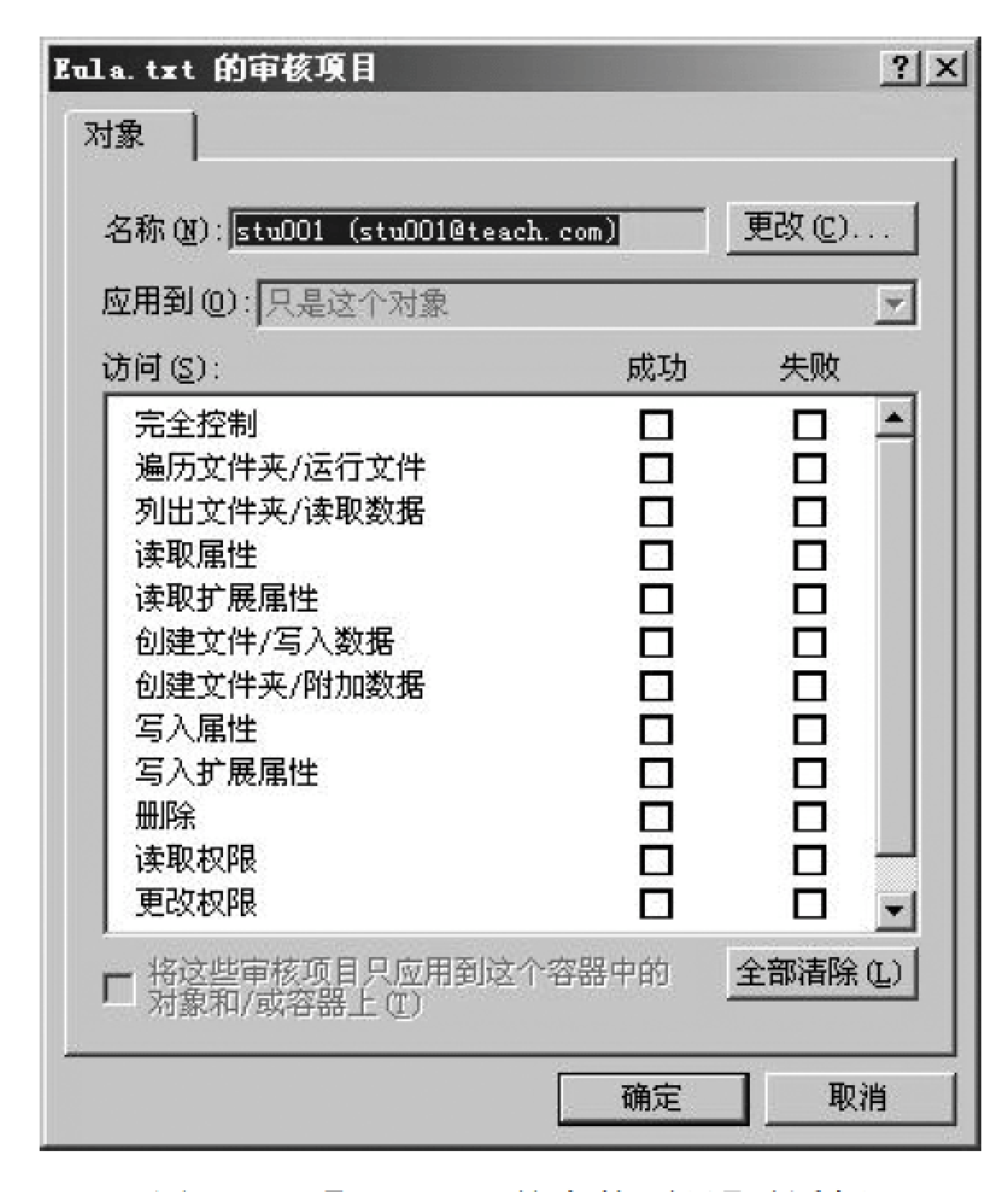


图 9-55 【Eula. txt 的审核项目】对话框



3．事件查看器

使用“事件查看器”，可以监视事件日志中记录的事件。通常，计算机会存储应用程序、安全性和系统日志。根据计算机的角色和所安装的应用程序，还可能包括其他日志，如目录服务、DNS 服务器、文件复制服务等。

提示：日志文件是一些文件系统集合，依靠建立起的各种数据的日志文件而存在。在任何系统发生崩溃或需要重新启动时，数据就遵从日志文件中的信息记录原封不动进行恢复。日志对于系统安全的作用是显而易见的，无论是网络管理员还是黑客都非常重视日志，一个有经验的管理员往往能够迅速通过日志了解到系统的安全性能。

打开事件查看器的方法为：选择【开始】/【程序】/【管理工具】/【计算机管理】命令，打开【计算机管理】窗口，在左侧窗口的目录树中，选择【计算机管理（本地）】/【系统工具】/【事件查看器】选项，打开【事件查看器】属性窗口（图 9-56）。



图 9-56　【事件查看器】属性窗口

（1）事件日志类型。事件查看器中各种日志的作用如下。

① 应用程序。记录应用程序或系统程序记录的事件。例如，数据库应用程序可能会将文件错误记录在应用程序日志中。

② 安全性。记录登录尝试以及与资源使用相关的事件。如有效的和无效的登录尝试，以及与创建、打开或删除文件等资源使用相关联的事件。

③ 系统。记录 Windows 系统组件记录的事件。例如，在启动过程将加载的驱动程序或其他系统组件的失败记录在系统日志中。

④ 目录服务。记录与 Active Directory 相关的事件。只有域控制器上提供此日志。

⑤ DNS 服务器。记录与 DNS 名称和 IP 协议地址双向解析相关的事件。只有 DNS 服务器上提供此日志。

⑥ 文件复制服务。记录域控制器之间进行复制过程中记录的事件。只有域控制器上提供此日志。



(2) 事件类型。事件查看器的事件类型有以下五种(其图标样式如图 9-57 所示)。

① 错误(红色图标)。重要的问题,如数据丢失或功能丧失。例如,如果在启动过程中某个服务加载失败,这个错误将会被记录下来。

② 警告(黄色图标)。并不是非常重要,但有可能说明将来的潜在问题的事件。例如,当磁盘空间不足时,将会记录警告。

③ 信息(白色图标)。描述了应用程序、驱动程序或服务的成功操作的事件。例如,当网络驱动程序加载成功时,将会记录一个信息事件。

④ 成功审核(锁匙图标)。成功的审核安全访问尝试。例如,用户试图登录系统成功会作为成功审核事件记录下来。

⑤ 失败审核(锁图标)。失败的审核安全登录尝试。例如,如果用户试图访问网络驱动器并失败了,则该尝试将会作为失败审核事件记录下来。

(3) 保存日志。各类事件日志可以以日志文件的形式保存。保存方法为:选择菜单栏的【操作】/【另存日志文件】命令(图 9-58)。日志文件的扩展名为.evt。



图 9-57　事件查看器的事件类型



图 9-58　菜单栏的【操作】/【另存日志文件】命令

9.8　域安全策略的应用

为了更好地说明域安全策略的作用,下面分别介绍账户策略设置、审核策略设置的实际应用。

9.8.1　账户策略设置

1. 案例背景

公司里很多职员设置密码比较草率,存在以下不安全因素:长度很短,而且不符合复杂性要求;密码从不更改;有时会发生非法用户试探职员密码,想窃取公司保密信息的情况。

2. 方案设计

设置域账户密码长度至少 8 个字符;密码符合复杂性要求;密码至少 45 天修改一次;输



入 5 次错误密码即锁定该用户账户。

3. 实施要求

进行上述策略设置，并验证策略的效果，试锁定某个用户账户，并为其解锁。

4. 操作步骤

(1) 以 Administrator 账户登录域控制器，选择【开始】/【程序】/【管理工具】/【域安全策略】命令，打开【默认域安全设置】窗口，在左侧窗口的目录树中，选择【Windows 设置】/【安全设置】/【账户策略】/【密码策略】选项，打开【密码策略】属性窗口(图 9-59)。

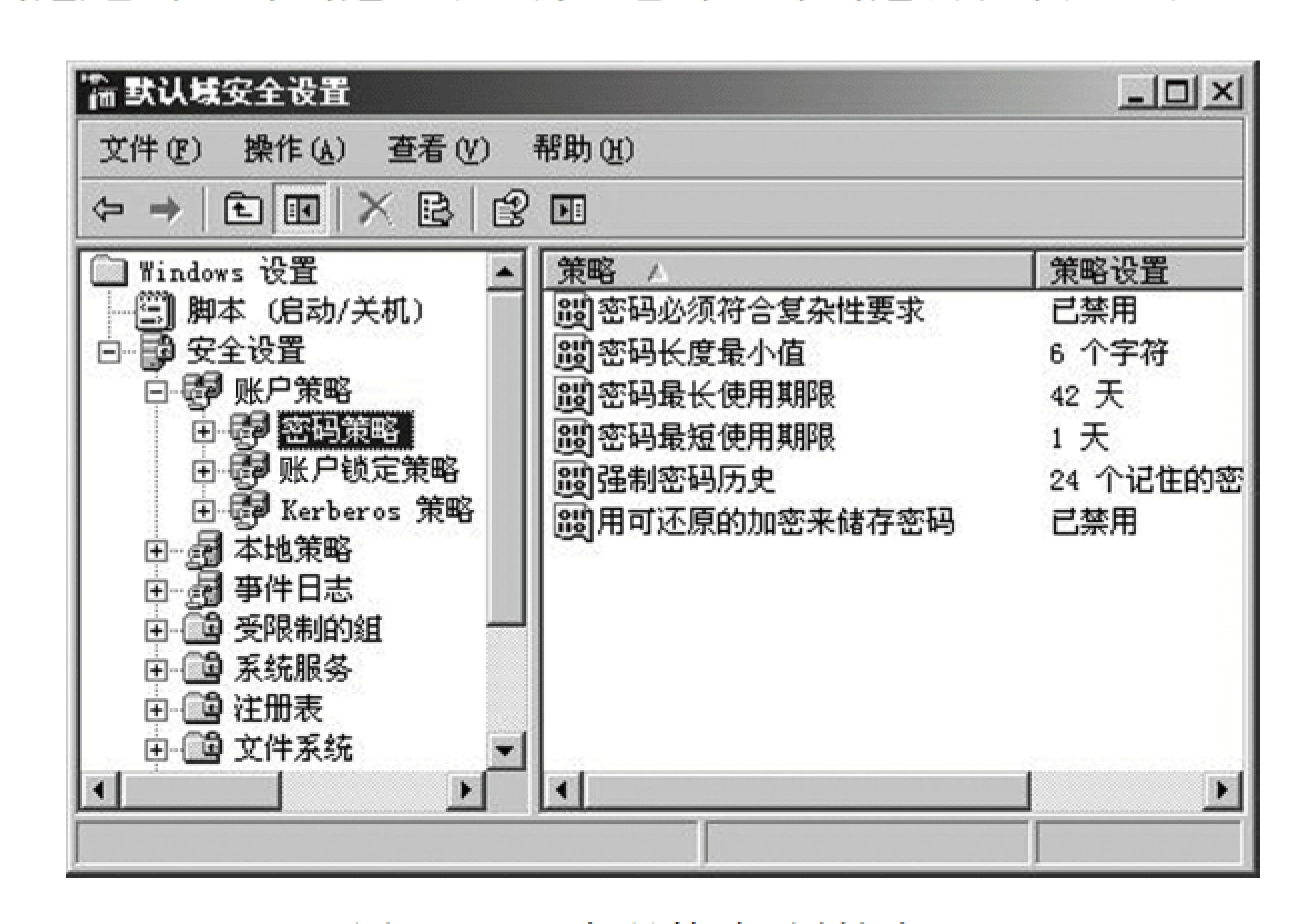


图 9-59　【密码策略】属性窗口

(2) 设置【密码长度最小值】选项的值为 8。详细操作步骤参考 9.5.3 小节。

(3) 双击【密码必须符合复杂性要求】选项，打开【密码必须符合复杂性要求 属性】对话框，选中【定义这个策略设置】复选择框，选择【已启用】单选按钮(图 9-60)，单击【确定】按钮即可。

(4) 双击【密码最长使用期限】选项，打开【密码最长使用期限 属性】对话框，选中【定义这个策略设置】复选择框，在【密码过期时间】文本框中输入 45(图 9-61)。单击【确定】按钮完成密码至少 45 天修改一次的设置。

(5) 在图 9-59 所示的窗口左侧，选择【账户锁定策略】选项，设置账户锁定阈值为 5。详细操作步骤参考 9.5.3 小节。

(6) 运行 gpupdate 命令刷新域安全策略。

提示：由于域的账户策略优先级最高，因此，只要修改域安全策略，不管域控制器安全策略设置如何，都可以保证对整个域的所有计算机生效。

(7) 修改某个账户(如 sale002)的密码，验证密码策略是否起作用。

(8) 使用某个域账户(如 sale002)登录客户端，故意输错密码，验证账户锁定策略是否起作用。

(9) 在域控制器上，由 Administrator 账户解除对被锁账户(如 sale002)的锁定。验证该账户能否正常登录。详细操作步骤可以参考 9.5.3 小节。



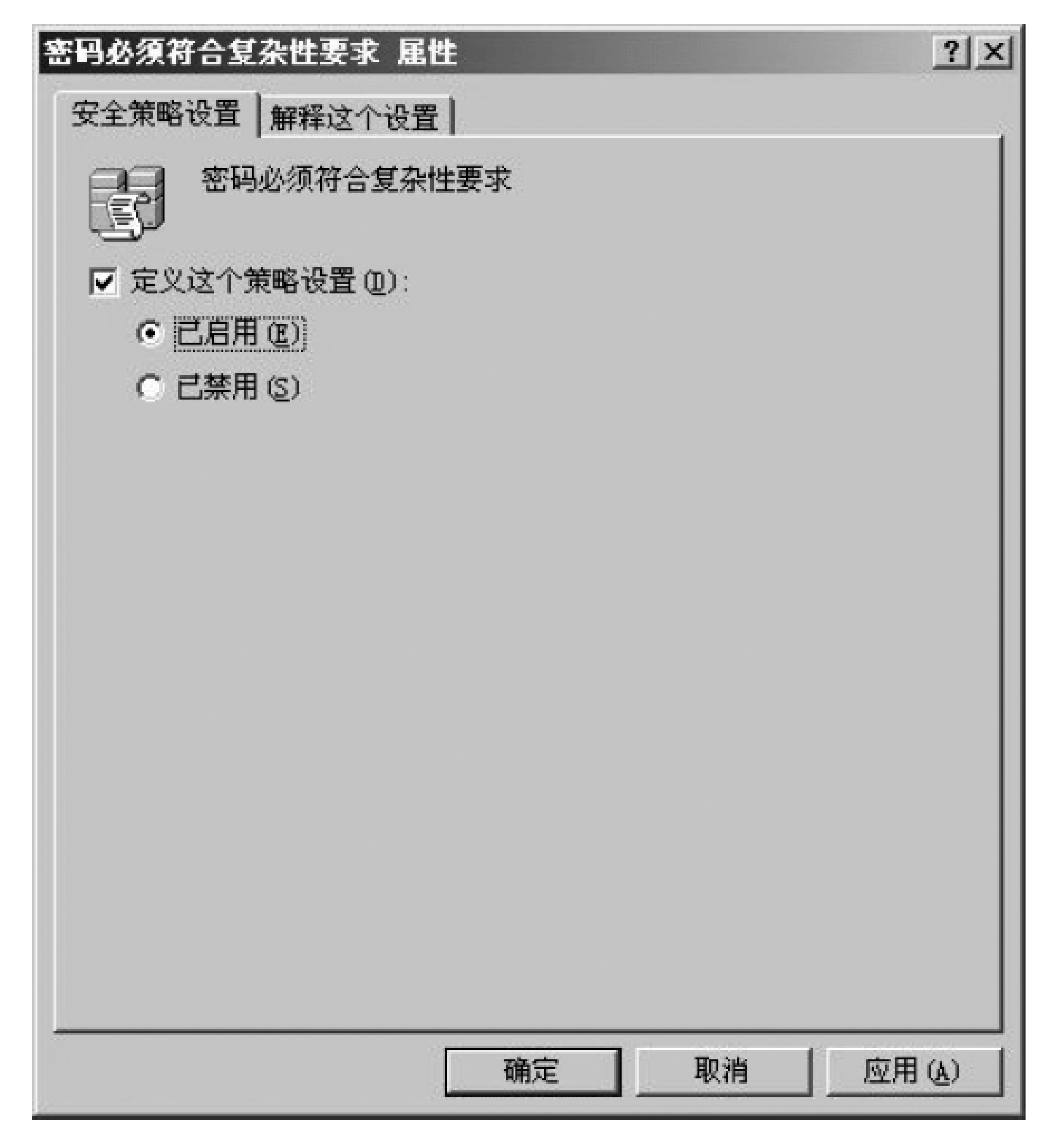


图 9-60 【密码必须符合复杂性要求 属性】对话框

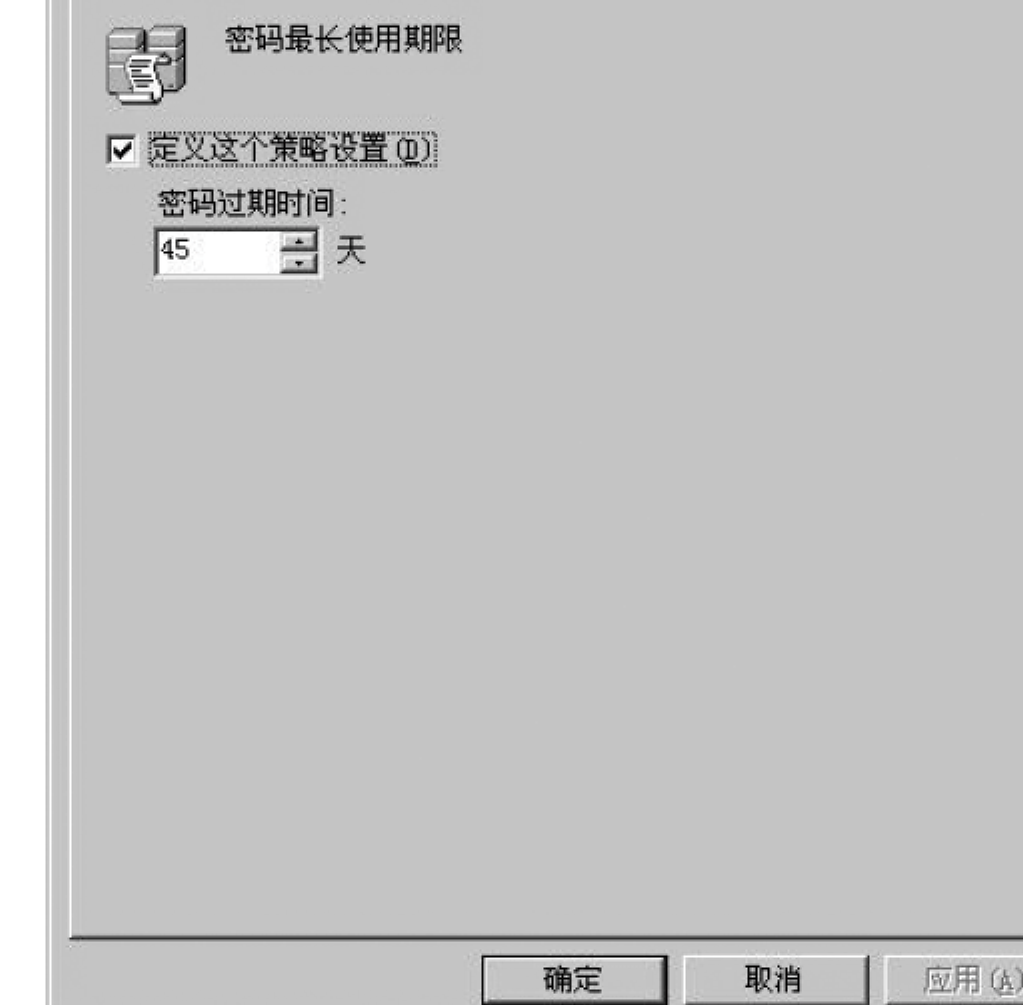


图 9-61 【密码最长使用期限 属性】对话框

9.8.2 审核策略设置

1. 案例背景

企业内部业务数据非常重要，非授权人员不能访问，但又需要在一定范围内共享。有时会发生非法用户尝试读取这些数据，想窃取公司保密信息的情况。管理员必须及时掌握这些非法用户的可疑行为，并采取相应措施，保证保密信息的安全性。

2. 方案设计

使用 EFS 对保密文件夹进行加密，并授予可访问的用户权限，然后启用 EFS 文件共享；设置审核策略，审核所有用户账户对保密文件夹的访问情况。

3. 实施要求

进行上述策略设置，并分别以授权用户账户和非授权用户账户登录系统，对保密文件夹进行访问，通过事件查看器了解记录情况。

4. 操作步骤

(1) 以 Administrator 账户登录域控制器，使用 EFS 对保密文件夹(如 C:\admini)加密，并授予可访问的用户(比如 info 组中的 info001 和 info002 账户)权限，然后启用 EFS 文件共享(详细操作步骤参考 8.3.4 小节)。设置该文件夹的共享属性，使之可以通过网络共享。





（2）选择【开始】/【程序】/【管理工具】/【域安全策略】命令，打开【默认域安全设置】窗口，在左侧窗口的目录树中，选择【Windows 设置】/【安全设置】/【本地策略】/【审核策略】选项，打开【审核策略】属性窗口（图 9-51）。

（3）在右侧详细信息列表窗格中双击【审核对象访问】选项，打开【审核对象访问 属性】对话框，选中【定义这些策略设置】复选框，选中【失败】和【成功】复选框（图 9-62）。单击【确定】按钮。



图 9-62　【审核对象访问 属性】对话框

（4）检查并修改域控制器安全策略，确保其相应安全选项的设置不会因为优先级高于域安全策略而阻止上述策略的实现。然后，运行 gpupdate 命令，刷新安全策略。

提示：为了保证域安全策略某些选项修改后能够生效，对域控制器安全策略必须采取下列两种方法中的一种进行设置：第一种方法，将域控制器安全策略相应选项设置为“未定义”，即取消对【定义……设置】复选框的选中，使该策略不起作用（图 9-63）。否则，会按照默认设置执行。第二种方法，将域控制器安全策略相应选项设置为与域安全策略相同。

（5）在需要审核的文件夹 C:\admini 上右击，在弹出的【admini 属性】对话框中选择【安全】选项卡，单击【高级】按钮，打开【admini 的高级安全设置】对话框。选择【审核】选项卡（图 9-63），单击【添加】按钮，参考 9.6.2 小节的步骤，添加要审核的账户（如 everone）。

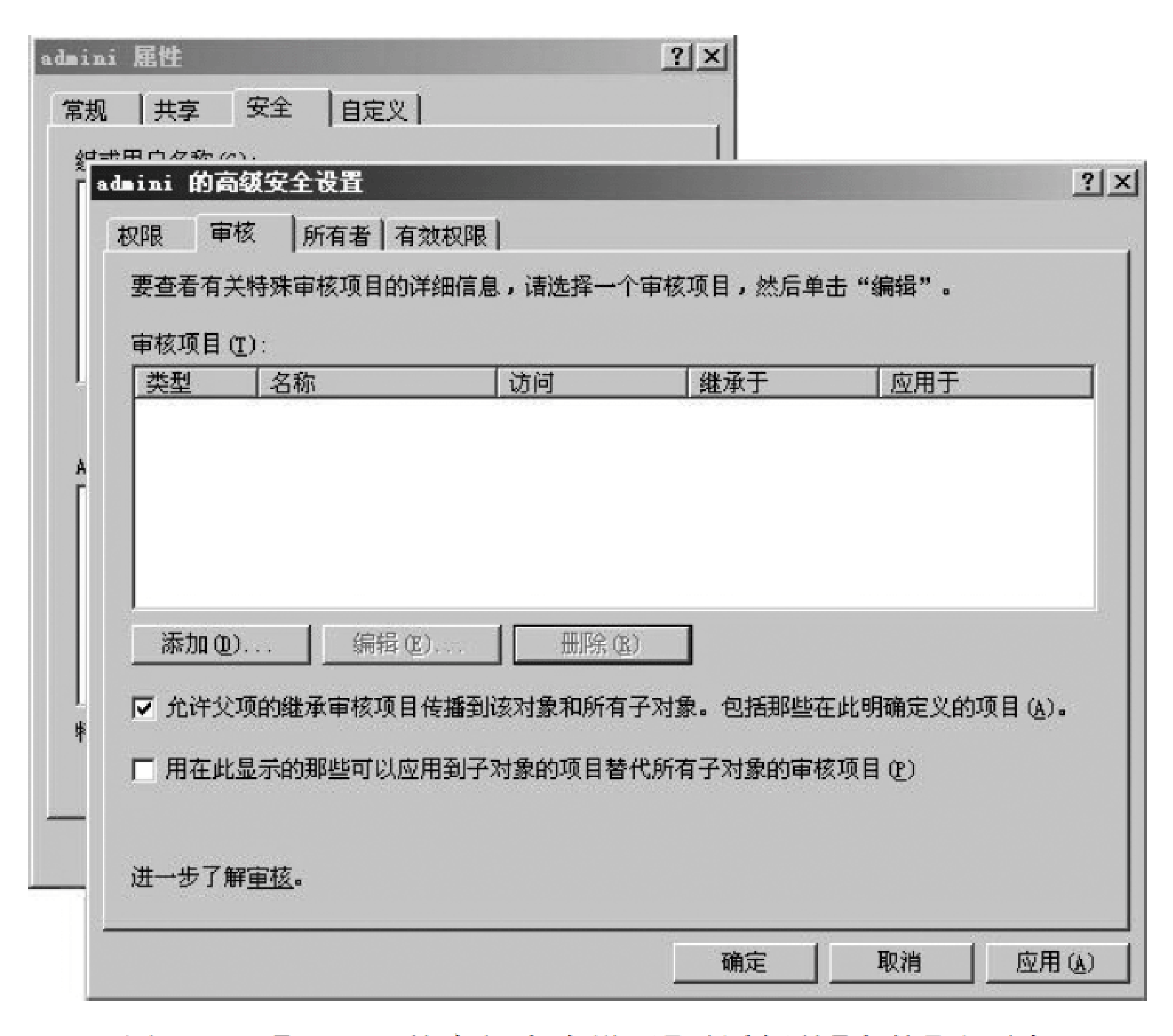


图 9-63　【admini 的高级安全设置】对话框的【审核】选项卡



(6) 单击两次【确定】按钮后，打开【admini 的审核项目】对话框，选中所有关于成功和失败的复选框(图 9-64)。单击【确定】按钮，返回上一级对话框，依次单击【确定】按钮，直到关闭所有对话框。设置完成。

(7) 以 info001 账户登录客户端，通过共享访问文件夹 C:\admini，并读取其中的文件 exam001.txt。结果可以成功读取。说明授权用户可以访问加密文件。

(8) 在域控制器中，打开事件查看器，在如图 9-56 所示的窗口中，选择左侧目录树中的【安全性】选项，可以在右侧详细信息列表窗格中看到对 info001 账户进行对象访问审核成功的记录(图 9-65)。双击相关记录，打开【事件属性】对话框，可以看到关于事件的详细信息(图 9-66)。

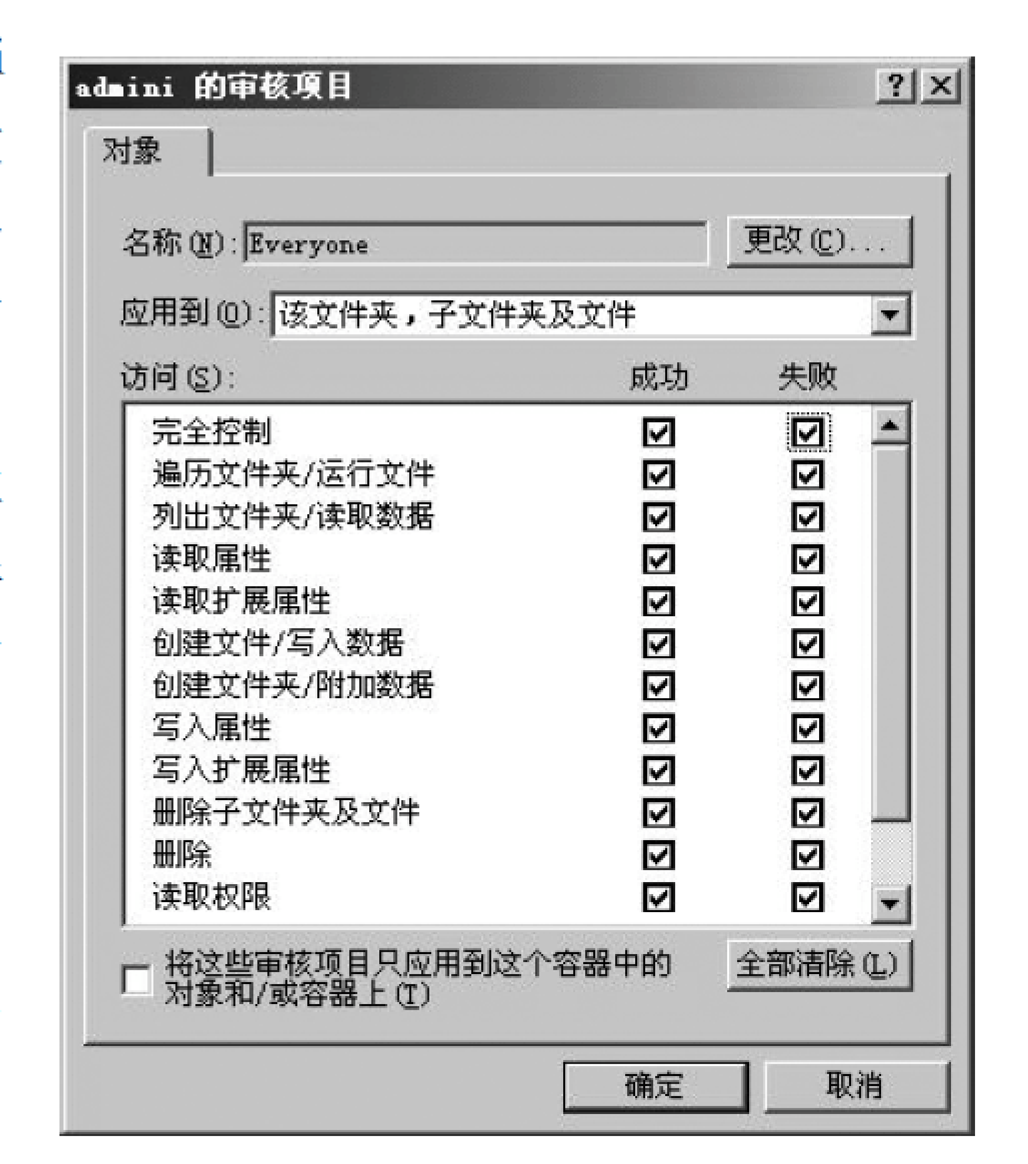


图 9-64 【admini 的审核项目】对话框

(9) 注销 info001 账户，以非授权用户账户(如 other002)登录客户端，通过共享访问文件夹 C:\admini，并读取其中的文件 exam001.txt。结果弹出拒绝访问提示对话框(图 9-67)，提示访问该文件失败。说明非授权用户无法访问加密文件。

(10) 在域控制器中，打开事件查看器，可以查看到对 other001 账户进行对象访问审核成功的记录及关于事件的详细信息(相关操作参考前面的步骤)。

提示：虽然 other001 账户不能读取文件夹 admini 中的文件，但是 other001 能成功访问到文件夹 admini，因此，事件查看器的【安全性】选项中有关“对象访问”审核成功的记录。



图 9-65 事件查看器【安全性】选项







图 9-66 【事件 属性】对话框



图 9-67 拒绝访问提示对话框

9.9 组策略概述

组策略是 AD 目录服务中的结构，可定义将自动应用到 AD 中的用户和计算机账户的默认设置。组策略常用于在用户或计算机集合上强制设置一些配置，使多台计算机具有统一的桌面环境、计算机启动/关机所执行的脚本文件、用户登录/注销所执行的脚本文件等。

组策略设置实际上就是修改注册表中的配置，不过，组策略使用了更完善的管理组织方法，比手工修改注册表要方便灵活得多，功能也更加强大。

组策略不仅应用于用户和客户端计算机，还应用于成员服务器、域控制器以及管理范围内的任何 Windows 2000/XP/Server 2003 计算机。组策略不会影响没有加入域的用户和计算机。

9.9.1 组策略的作用

(1) 方便地管理 AD 中的计算机和用户。包括用户桌面环境设置、计算机启动/关机与用户登录/注销时所执行的脚本文件、软件分发、软件限制、安全设置等。组策略通过活动目录可以对域中的用户和计算机进行管理(图 9-68)。

(2) 对域设置组策略，可以影响整个域的工作环境；对 OU 设置组策略，可以影响 OU 下的工作环境。

(3) 提高工作效率，防止不正确的配置。组策略只需要设置一次，相应的用户或计算机就可以全部使用规定的配置，同时防止用户不正确配置环境的情况。

(4) 推行计算机使用规范。通过组策略的设置，统一用户桌面规范、统一实施安全策略。



9.9.2 组策略的结构

组策略的结构如图 9-69 所示。说明如下。

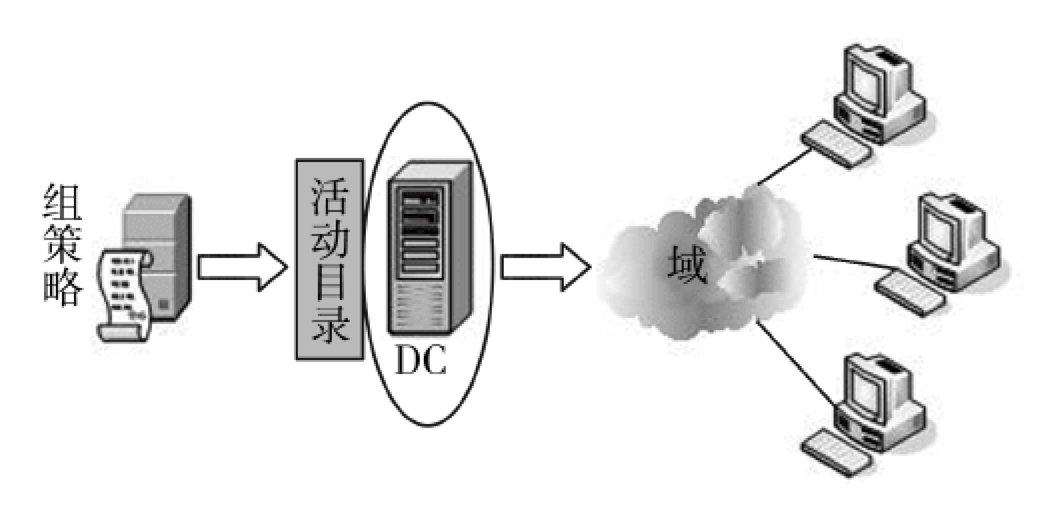


图 9-68 组策略对计算机和用户的管理方式

GPO
SDOU
计算机
用户
组策略

图 9-69 组策略结构图

(1) 组策略的具体设置数据保存在 GPO 中。GPO(Group Policy Object,组策略对象)是组策略设置的集合,实质上是由组策略对象编辑器创建的文档。

(2) 系统有两个默认的 GPO:默认域策略和默认域控制器策略。默认域策略与域连接,通过策略继承影响域中所有用户和计算机(包括作为域控制器的计算机)。

默认域控制器策略与域控制器 OU 链接,只影响域控制器,因为域控制器的用户和计算机单独保存在域控制器 OU 中。

(3) GPO 所链接的对象是 SDOU。即 Site(站点)、Domain(域)和 Organizational Unit(组织单位)。

AD 中的站点是从物理上抽象的概念,由一个或几个通过高速连接在一起的 IP 子网组成。一个站点可以包括多个域,一个域中也可以包括多个站点。站点的主要作用是优化复制,使用户能使用可靠、高速的连接登录到域控制器上。

(4) GPO 控制 SDOU 中的用户和计算机。

9.9.3 组策略对象及其存储

1. 组策略对象

有两种组策略对象:本地组策略对象和非本地组策略对象。

(1) 本地组策略对象。任何运行 Windows 2000/XP/Server 2003 操作系统的计算机都只有一个本地组策略对象。在这些对象中,组策略设置存储在各个计算机上,无论它们是否属于 AD 环境或网络环境的一部分。

在 AD 环境中,本地组策略的设置可以被非本地组策略的设置覆盖。因此,在 AD 环境中其影响力很小。而在无 AD 的环境中,本地组策略的设置就非常重要。

打开本地 GPO 有以下两种方法。

方法一:选择【开始】/【运行】命令,在弹出的【运行】对话框中输入 MMC。打开【控制台 1】窗口(图 9-70),在菜单栏选择【文件】/【添加/删除管理单元】命令,打开【添加/删除管理单元】对话框(图 9-71),单击【添加】按钮,打开【添加独立管理单元】对话框(图 9-72),在列表中选择需要添加的管理单元,然后单击【添加】按钮,执行多次选择与添加操作,将需要添加的管理单



元添加到控制台中，然后单击【关闭】按钮。返回上一级对话框，单击【确定】按钮，返回【控制台 1】窗口，可以看到添加的管理单元出现在控制台树中（图 9-73）。在菜单栏选择【文件】/【保存】命令，可以保存控制台 1。或者在菜单栏选择【文件】/【另存为】命令，将控制台保存到更容易查找的地方（如我的文档），起一个更容易辨认的名字（如本地 GPO 控制台）。

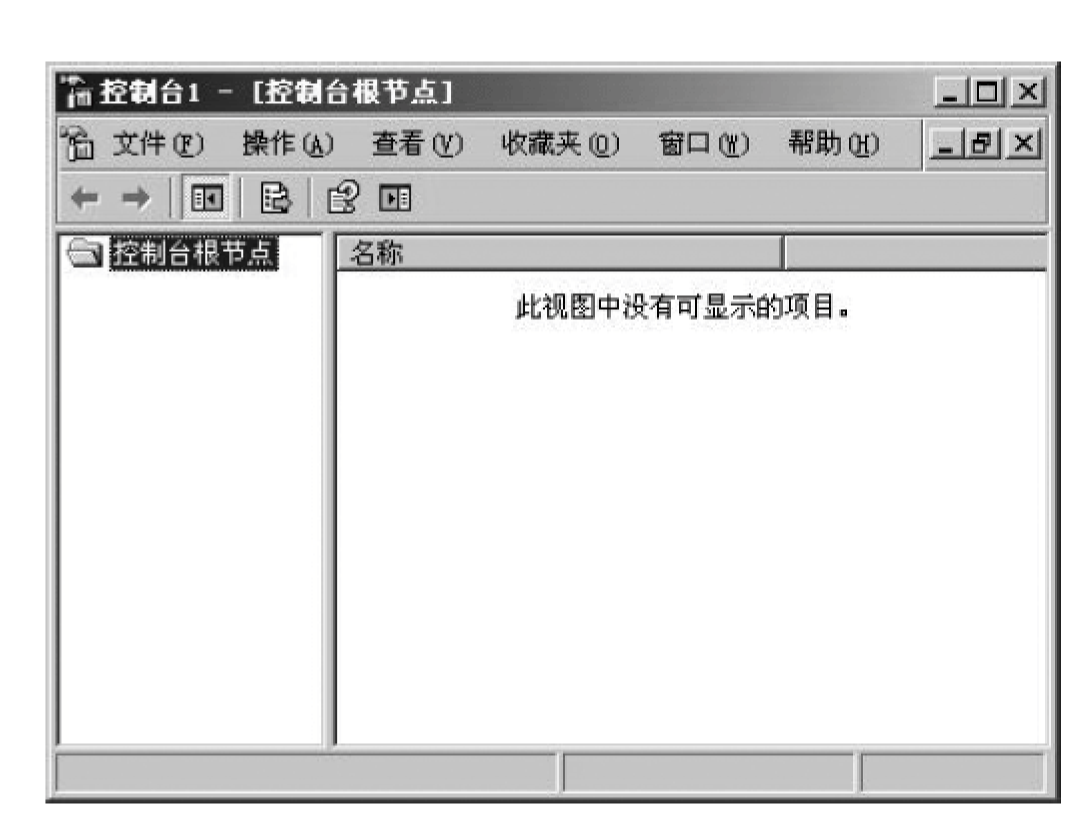


图 9-70 【控制台 1】窗口



图 9-71 【添加/删除管理单元】对话框



图 9-72 【添加独立管理单元】对话框

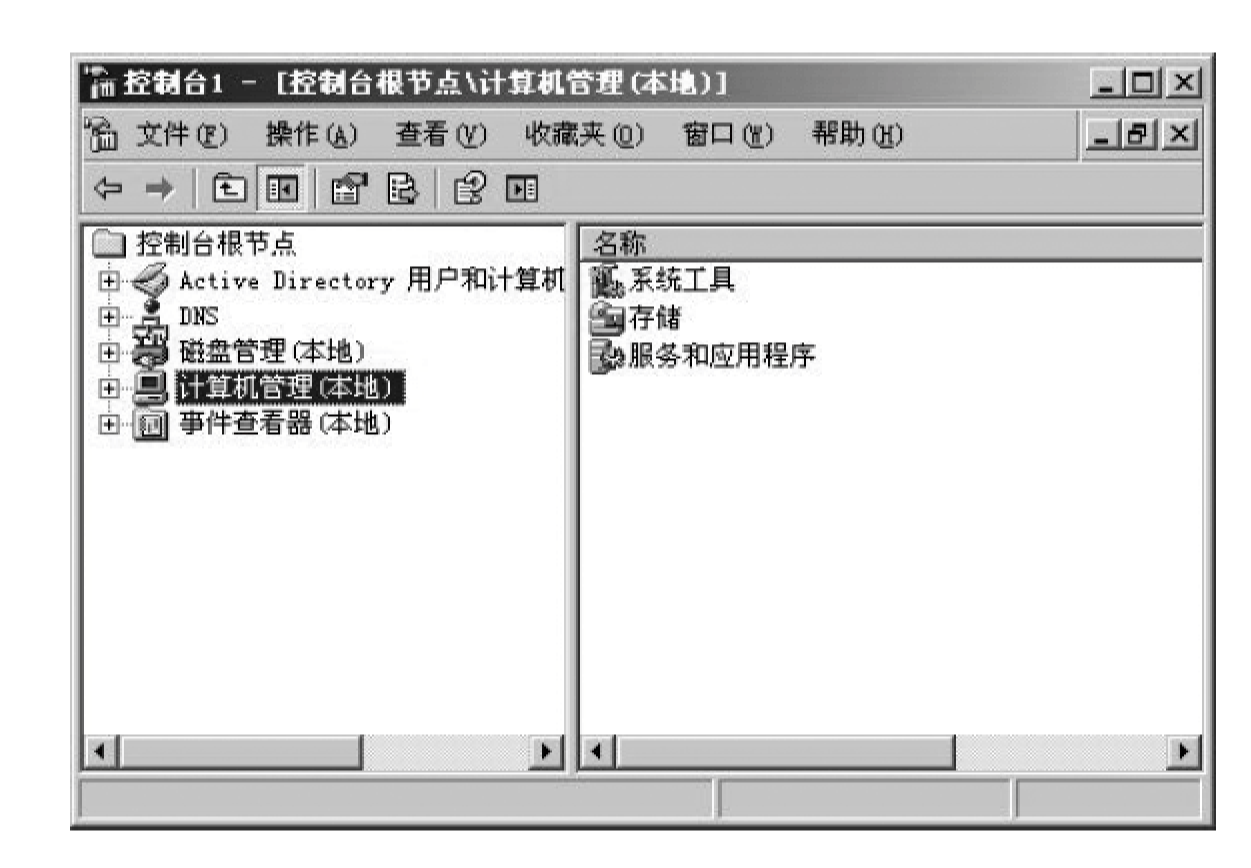


图 9-73 添加管理单元后的【控制台 1】窗口

这种方法可以按需要添加管理单元到控制台进行集中管理。

方法二：选择【开始】/【运行】命令，在弹出的【运行】对话框中输入 gpedit.msc 命令。

打开【组策略编辑器】窗口（图 9-74），在左侧目录树中包括了所有本地计算机策略选项。

（2）非本地组策略对象。存储在 DC 中的非本地组策略对象只能在 AD 环境下使用。它们可以影响到与组策略对象相关联的站点、域和 OU 中的用户和计算机。

2. 组策略对象的存储

GPO 的策略设置信息存储在两个位置：组策略容器和组策略模板。组策略容器是包含 GPO 属性和版本信息的活动目录对象；组策略模板是 GPO 存储域的域控制器文件夹。



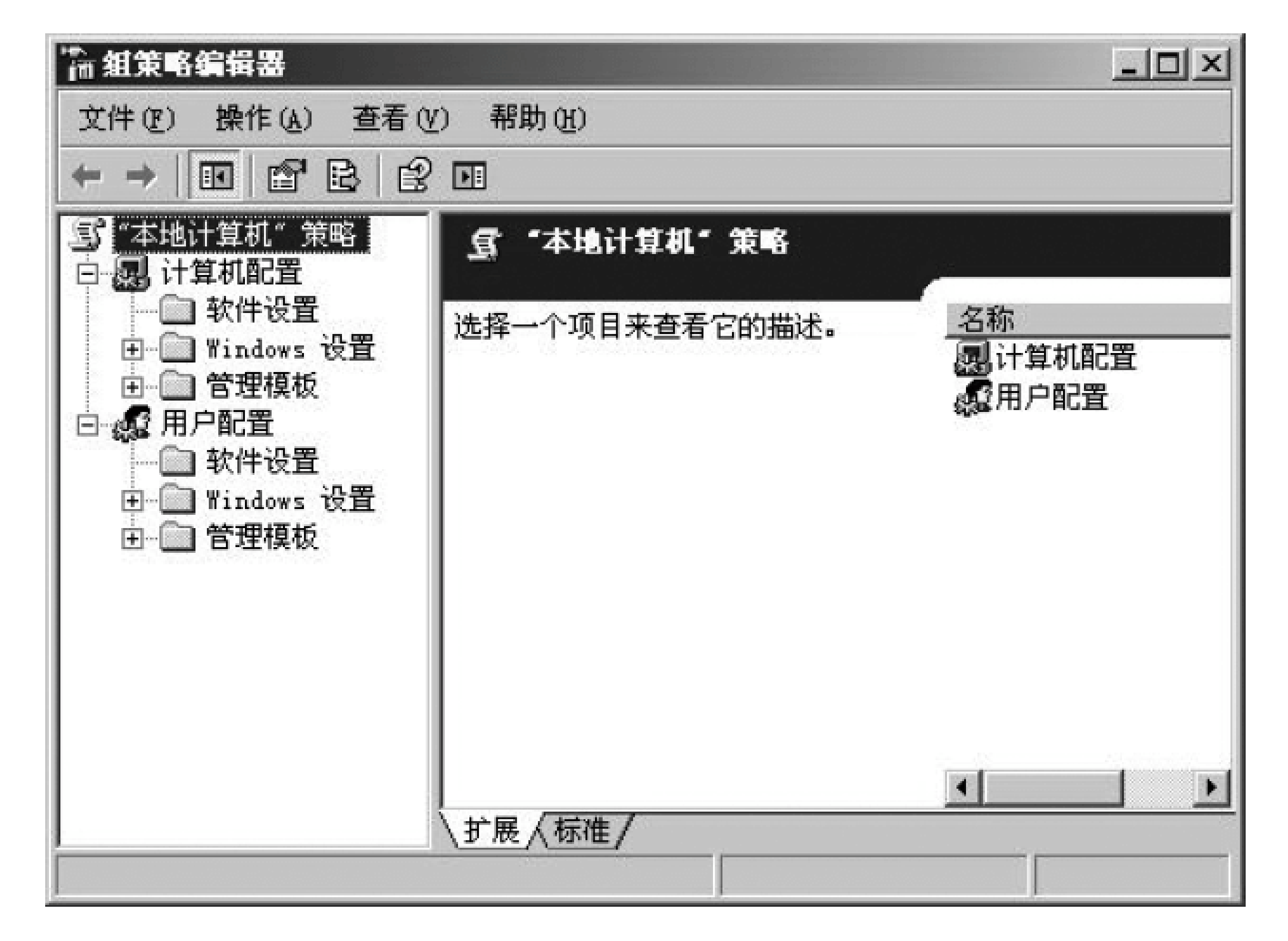


图 9-74 【组策略编辑器】窗口

9.9.4 组策略配置类型

应用组策略时存在两种配置类型：计算机配置和用户配置。

1. 计算机配置

计算机配置用于管理控制计算机特定项目的策略，包括桌面外观、安全设置、操作系统下运行、文件部署、应用程序分配、计算机启动和关机脚本运行。这些配置应用到特定的计算机上，当该计算机启动后，自动应用设置的组策略。

打开方式为：选择【开始】/【程序】/【管理工具】/【Active Directory 用户和计算机】命令，打开【Active Directory 用户和计算机】窗口（图 9-75），在域名（如 teach. com）上右击，在弹出的快捷菜单上选择【属性】命令，打开【teach. com 属性】对话框，选择【组策略】选项卡（图 9-76）。单击【编辑】按钮，打开【组策略编辑器】窗口（图 9-77），在左侧窗口的目录树中，可以看到计算机配置选项。



图 9-75 【Active Directory 用户和计算机】窗口







图 9-76　【teach.com 属性】对话框



图 9-77　【组策略编辑器】窗口

计算机配置包括下面三种设置。

(1) 软件设置。包含适用于登录到该计算机的所有用户的软件设置，主要包括软件安装设置。

(2) Windows 设置。包含适用于登录到该计算机的所有用户的 Windows 设置，主要包括脚本和安全设置，详细选项如图 9-78 所示。

(3) 管理模板。管理模板包含注册表设置，其详细选项如图 9-79 所示。

2. 用户配置

用于管理控制更多用户特定项目的管理策略，包括应用程序配置、桌面配置、应用程序



分配、计算机启动和关机脚本运行等。当用户登录到计算机时，就会应用用户配置组策略。当计算机配置和用户配置发生冲突时，用户策略将覆盖计算机策略。

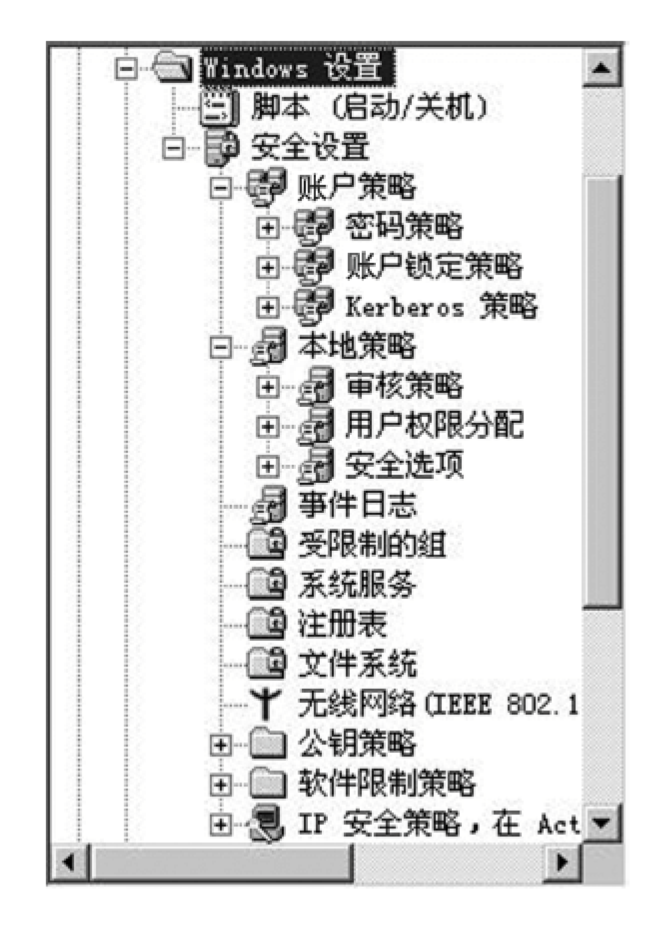


图 9-78 【计算机配置】的【Windows 设置】选项



图 9-79 【计算机配置】的【管理模板】选项

参考 1“计算机配置”的步骤打开如图 9-77 所示的窗口，在左侧窗口目录树中，可以看到用户配置选项。

（1）软件设置。无论用户使用哪台计算机都适用的软件设置，主要包括软件安装设置。

（2）Windows 设置。无论用户使用哪台计算机都适用的 Windows 设置，其详细选项如图 9-80 所示。

（3）管理模板。管理模板包含注册表设置，其详细选项如图 9-81 所示。

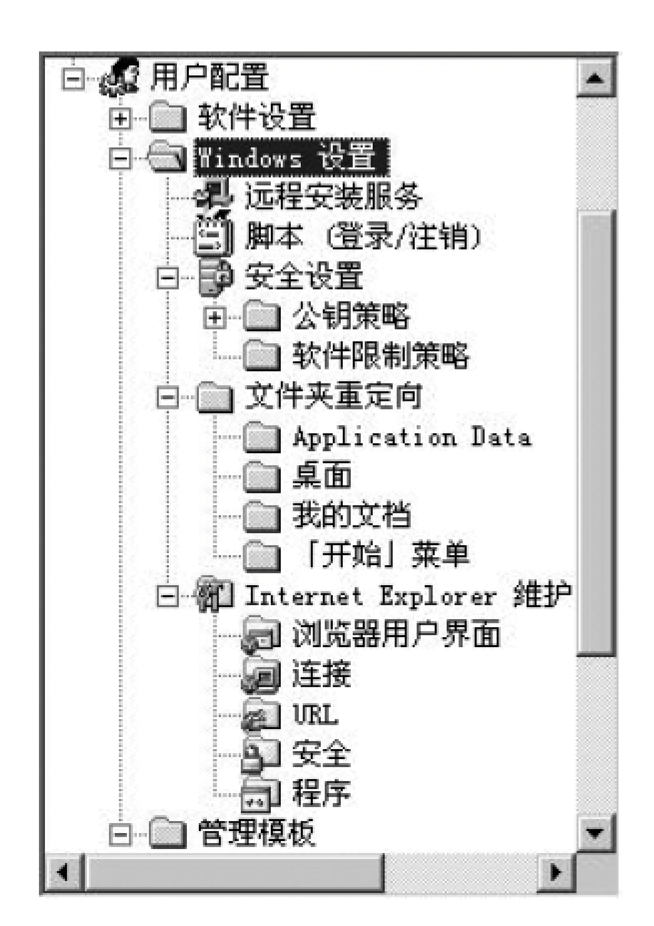


图 9-80 【用户配置】的【Windows 设置】选项

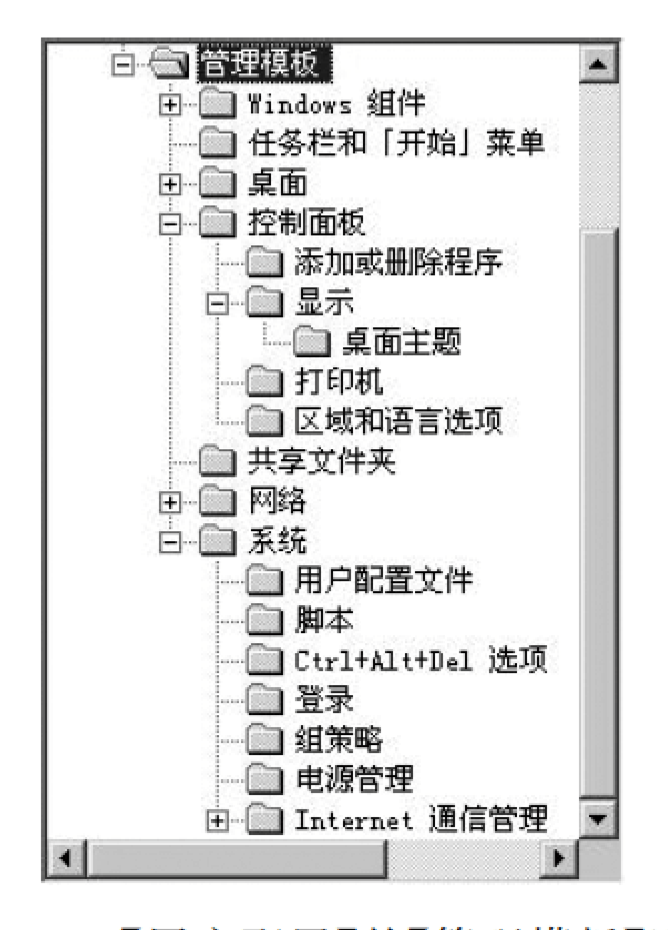


图 9-81 【用户配置】的【管理模板】选项

9.10 组策略对象的管理

组策略对象（GPO）的管理包括创建组策略、设置组策略、委托 GPO 管理控制、链接已存在的 GPO、删除 GPO 链接、删除 GPO。



9.10.1　创建组策略

每台计算机只有一个本地组策略，对于本地组策略只能编辑，无法创建。而对于域或OU，可以创建多个组策略。创建OU的组策略的步骤如下：

(1) 以Administrator账户登录系统（建议采用Windows Server 2003 R2 EnterPrise Edition），选择【开始】/【程序】/【管理工具】/【Active Directory用户和计算机】命令，打开【Active Directory用户和计算机】窗口（图9-82）。在teach.com域中添加名为stuOU的组织单位。



图9-82　【Active Directory用户和计算机】窗口

(2) 在左侧窗口的目录树中，选择需要创建组策略的stuOU组织单位，右击，在弹出的快捷菜单中选择【属性】命令（图9-83），打开【stuOU属性】对话框，选择【组策略】选项卡（图9-84）。



图9-83　选择stuOU组织单位的【属性】命令



(3) 单击【新建】按钮，在【组策略对象链接】文本框中输入新的组策略名称：stuOU Policy(图 9-85)，即创建了一个名为 stuOU Policy 的 GPO。单击【确定】按钮完成设置，即将 stuOU Policy 组策略应用到 stuOU 组织单位。



图 9-84 【stuOU 属性】对话框的【组策略】选项卡

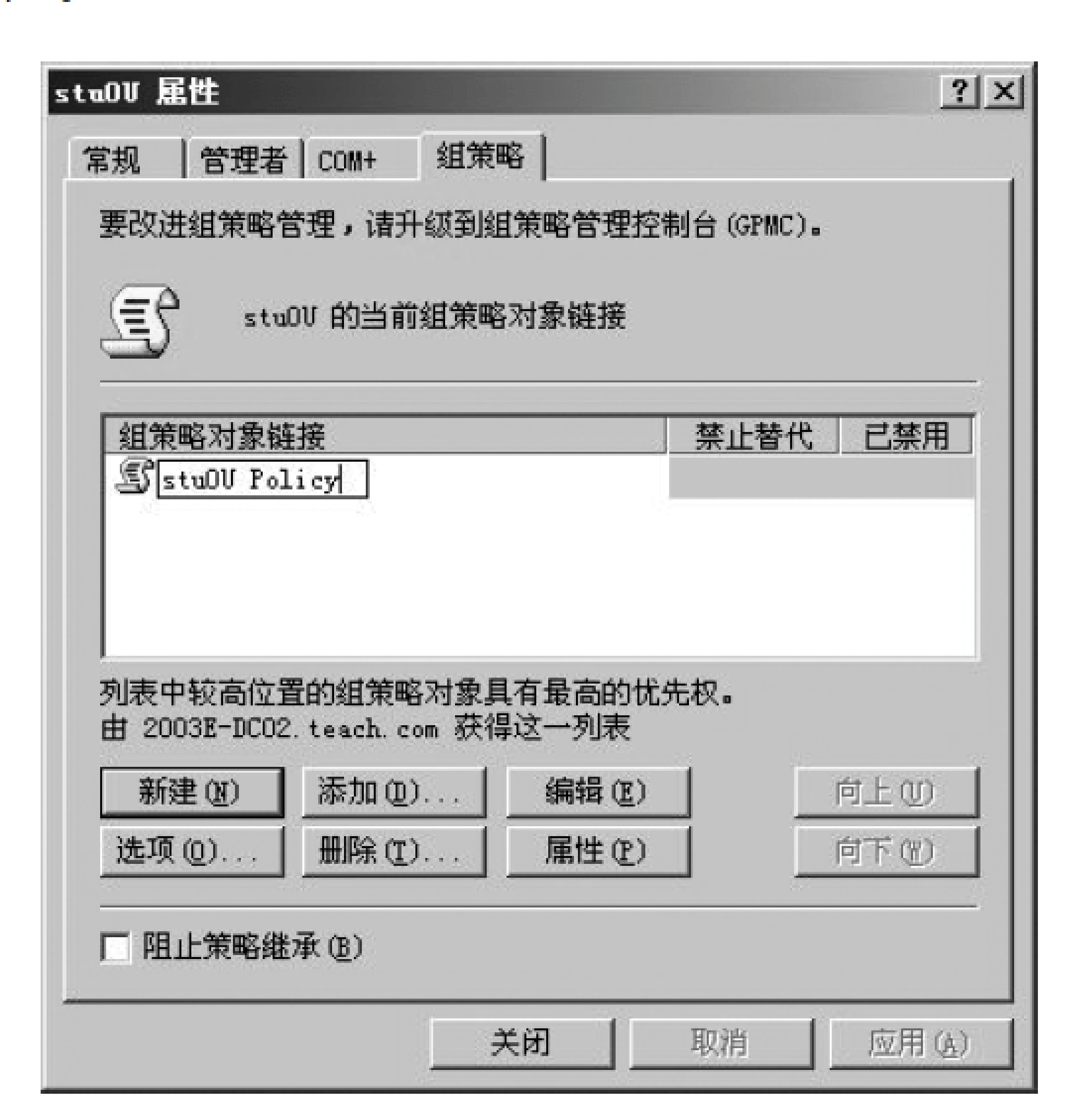


图 9-85 输入组策略名称：stuOU Policy

9.10.2 设置组策略

创建了 GPO 后，需要对该 GPO 进行设置。配置 GPO 的步骤如下：

(1) 在如图 9-85 所示的【stuOU 属性】对话框中，选择 stuOU Policy 组策略对象，单击【编辑】按钮，打开【组策略编辑器】窗口(图 9-86)。在左侧窗口的目录树中，可以选择自己需要设置的策略选项。



图 9-86 【组策略编辑器】窗口(一)



（2）例如想禁止 stuOU 组织单位中所有用户更改墙纸。则在左侧窗口的目录树中，选择【stuOU Policy】/【用户配置】/【管理模板】/【控制面板】/【显示】选项，在右侧详细信息列表窗格中选择【阻止更改墙纸】选项（图 9-87）。从图中【状态】栏可以看到该选项状态为“未被配置”。



图 9-87　【组策略编辑器】窗口(二)

（3）双击该选项，打开【阻止更改墙纸 属性】对话框，选择【已启用】单选按钮（图 9-88），单击【确定】按钮完成设置。返回如图 9-87 所示的窗口，可以看到该选项的状态已改为“已启用”。关闭【组策略编辑器】窗口，关闭【stuOU 属性】对话框。

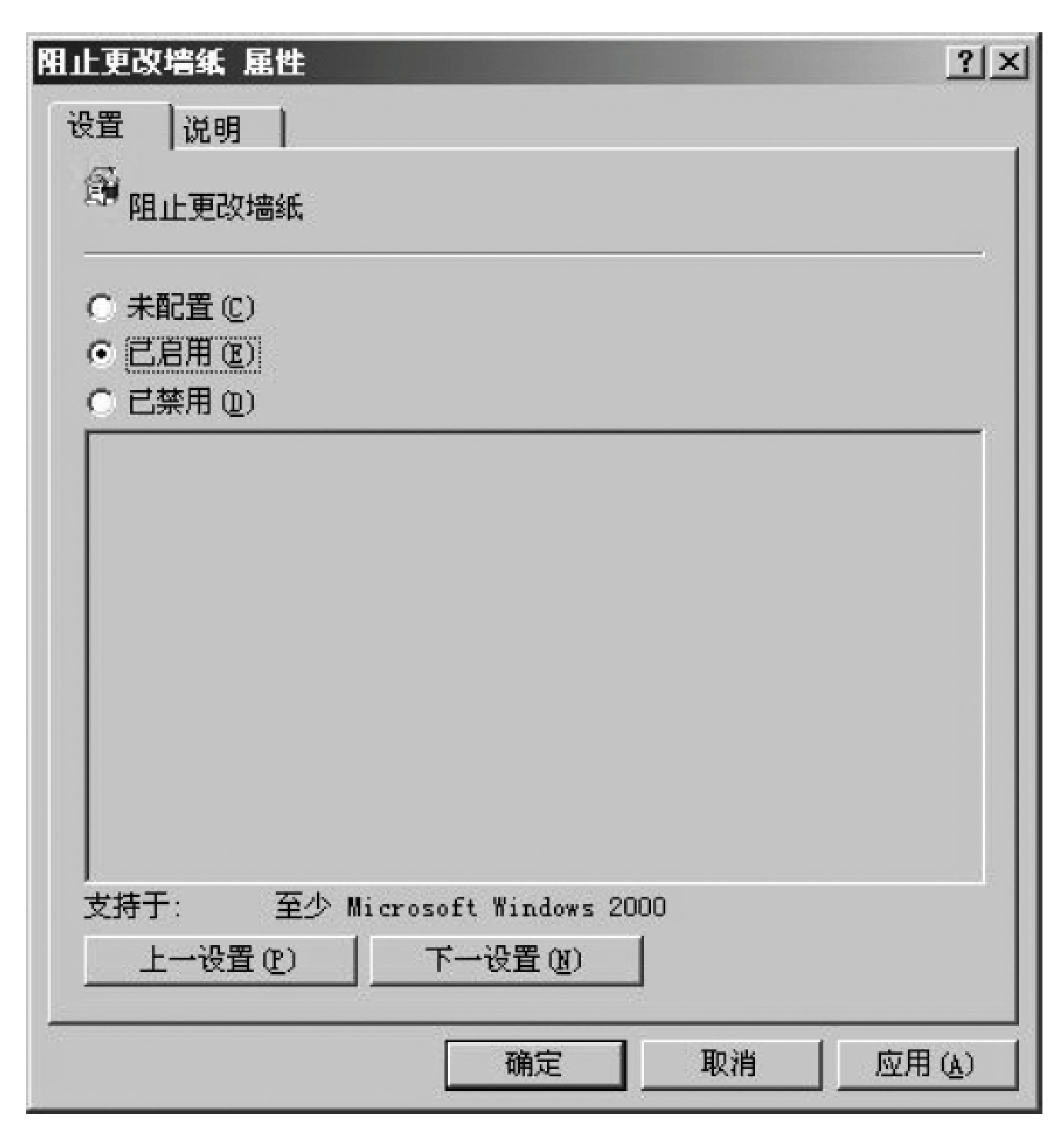


图 9-88　【阻止更改墙纸 属性】对话框



（4）运行 gpupdate 命令，刷新组策略。

（5）将 stu001 账户移动到 stuOU 组织单位中。打开如图 9-82 所示【Active Directory 用户和计算机】窗口，在右侧详细信息列表窗格中选择 stu001 账户，右击，在弹出的快捷菜单中选择【移动】命令（图 9-89）。打开【移动】对话框，选择 stuOU 选项（图 9-90），单击【确定】按钮完成设置。返回【Active Directory 用户和计算机】窗口，在左侧目录树中选择 stuOU 组织单位，在右侧详细信息列表窗格中可以看到 stu001 账户已被移动到该 OU 中（图 9-91）。



图 9-89　在 stu001 账户快捷菜单中选择【移动】命令



图 9-90　【移动】对话框



图 9-91　将 stu001 账户移动到 stuOU 组织单位中

（6）以 stu001 账户登录客户端，尝试更改桌面墙纸，结果失败。验证了组策略的作用。

9.10.3　委托 GPO 管理控制

创建并设置 GPO 后，需要确定哪些用户和组对 GPO 拥有访问权限。默认的 GPO 权



限如下：

- CREATOR OWNER 组：拥有特别的权限。
- Authenticated Users 组：拥有读、应用组策略和特别的权限。
- Domain Admins 组：拥有读、写、创建所有子对象、删除所有子对象、特别的权限。
- SYSTEM 组：拥有读、写、创建所有子对象、删除所有子对象、特别的权限。

如果需要委托某用户（如 info001）对 teach Policy 组策略有读取和应用组策略的权限。详细操作步骤如下：

（1）打开如图 9-85 所示【stuOU 属性】对话框，选择 stuOU Policy 组策略对象，单击【属性】按钮，打开【stuOU Policy 属性】对话框，选择【安全】选项卡（图 9-92）。

（2）单击【添加】按钮，参考 9.6.2 小节的步骤，添加 info001 账户。单击【确定】按钮，返回【stuOU Policy 属性】对话框，选中【info001 的权限】列表中的“读取”和“应用组策略”选项的【允许】复选框（图 9-93）。单击【确定】按钮返回上一级对话框，单击【确定】按钮完成对 info001 账户委托组策略管理的设置。



图 9-92　【stuOU Policy 属性】对话框的【安全】选项卡

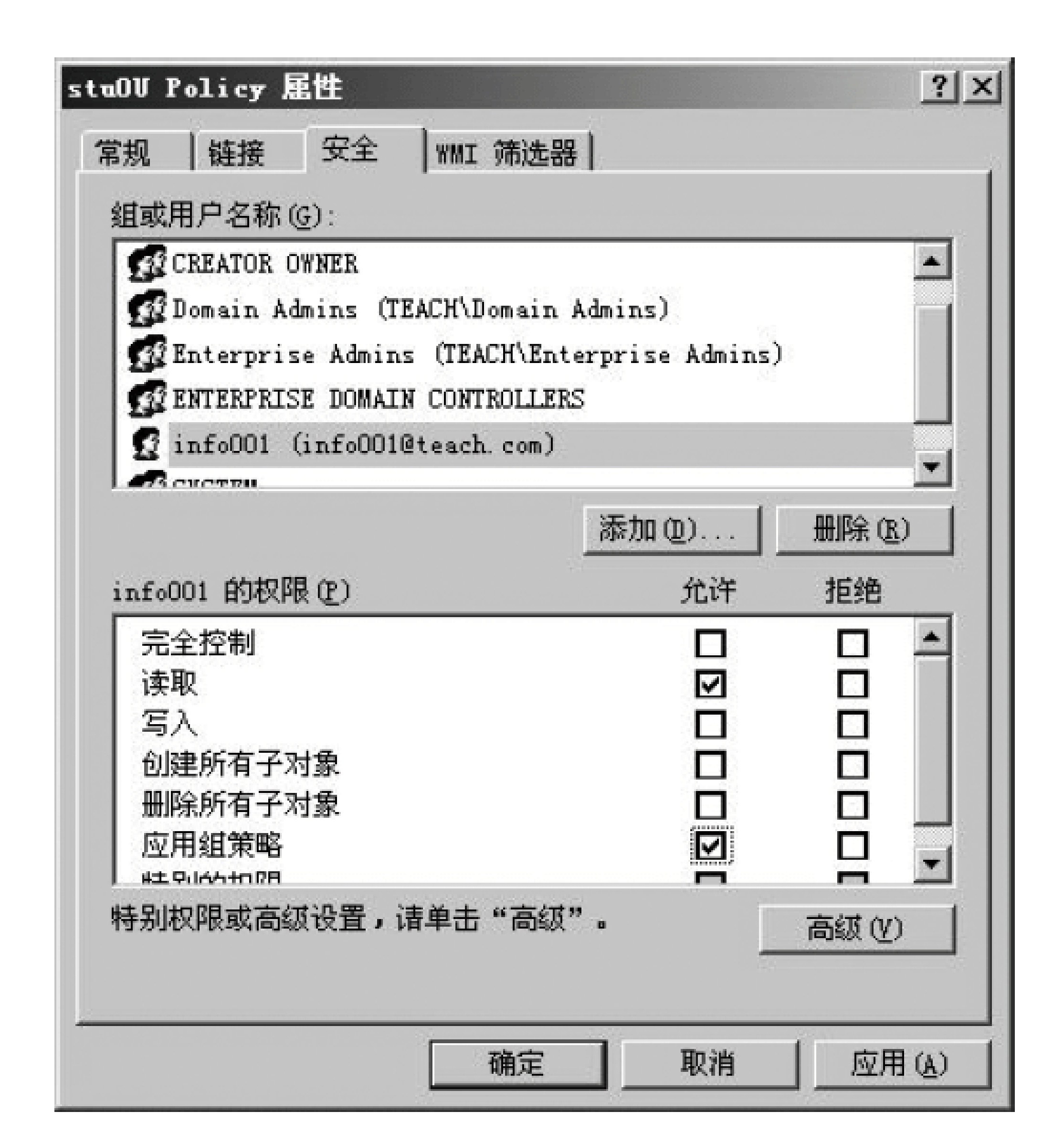


图 9-93　选中相应选项的【允许】复选框

提示：可以使用【添加】或【删除】按钮来添加或删除对组策略有权限的用户或组；也可以通过对【允许】或【拒绝】复选框的选中或取消选择操作，更改相应用户或组的权限。

（3）运行 gpupdate 命令，刷新组策略。

9.10.4　链接已存在的 GPO

如果已经建立了组策略，要将组策略应用到某个计算机或用户上，则通过链接 GPO 操作，将组策略应用到站点、域或组织单位中。例如将 stuOU Policy 组策略链接到 saleOU 组织单位。详细操作步骤如下：

（1）打开如图 9-82 所示的【Active Directory 用户和计算机】窗口，在 teach.com 中添加



名为 saleOU 的组织单位。选择该组织单位，右击，在弹出的快捷菜单中选择【属性】命令，打开【saleOU 属性】对话框，选择【组策略】选项卡（图 9-94）。

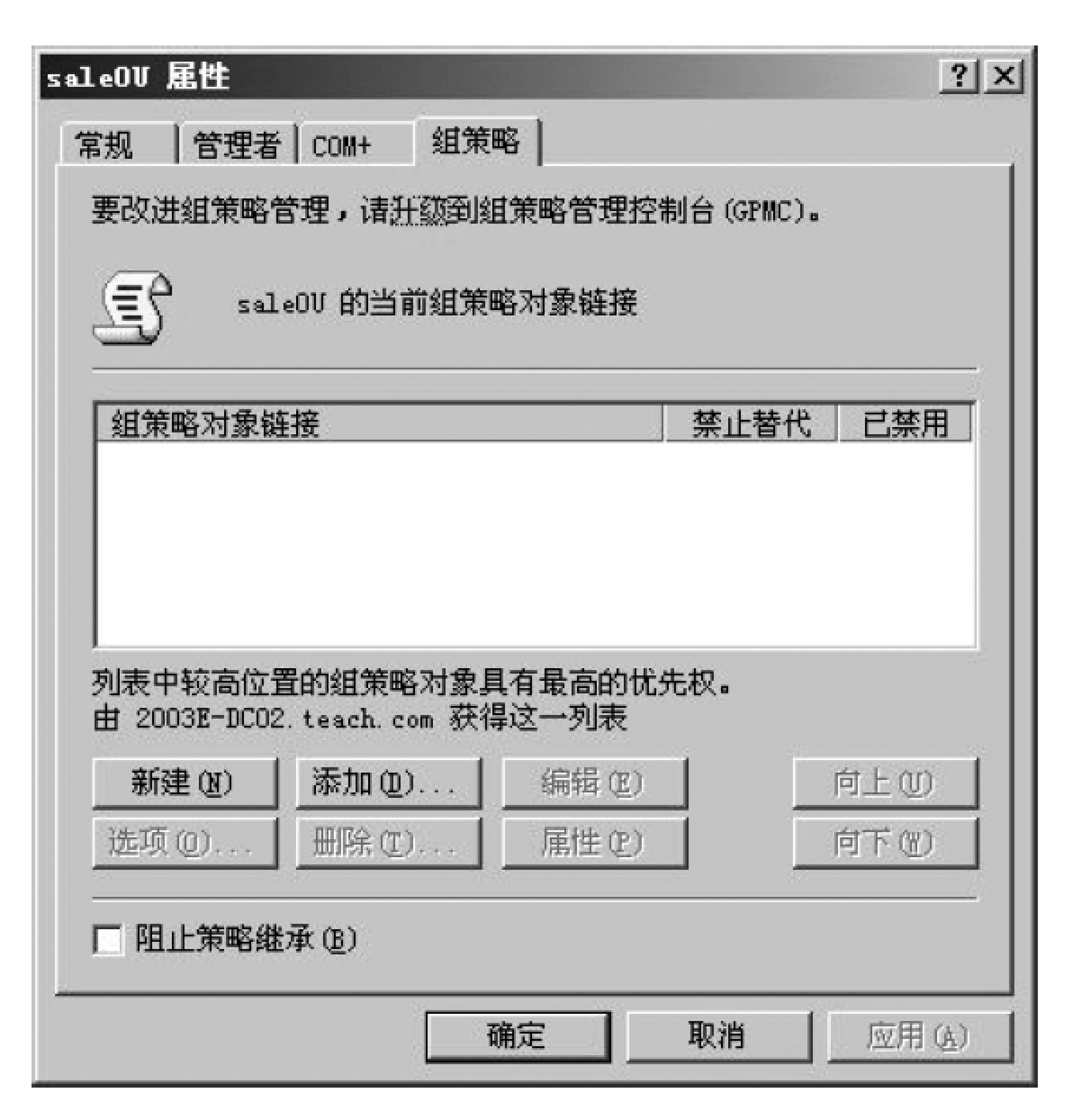


图 9-94 【saleOU 属性】对话框的【组策略】选项卡

（2）单击【添加】按钮，打开【添加组策略对象链接】对话框，选择【全部】选项卡（图 9-95）。在【存储在本域中的所有组策略对象】列表中选择要链接的组策略对象 stuOU Policy，单击【确定】按钮，返回【saleOU 属性】对话框，可以看到该 GPO 出现在【saleOU 的当前组策略对象链接】列表框中（图 9-96）。

（3）单击【确定】按钮，完成设置。

（4）运行 gpupdate 命令，刷新组策略。

（5）验证。参考 9.10.2 小节的步骤，将 sale001 账户移动到 saleOU 组织单位中。以 sale001 账户登录客户端，尝试更改桌面墙纸，结果失败。证明成功链接了已存在的 GPO。

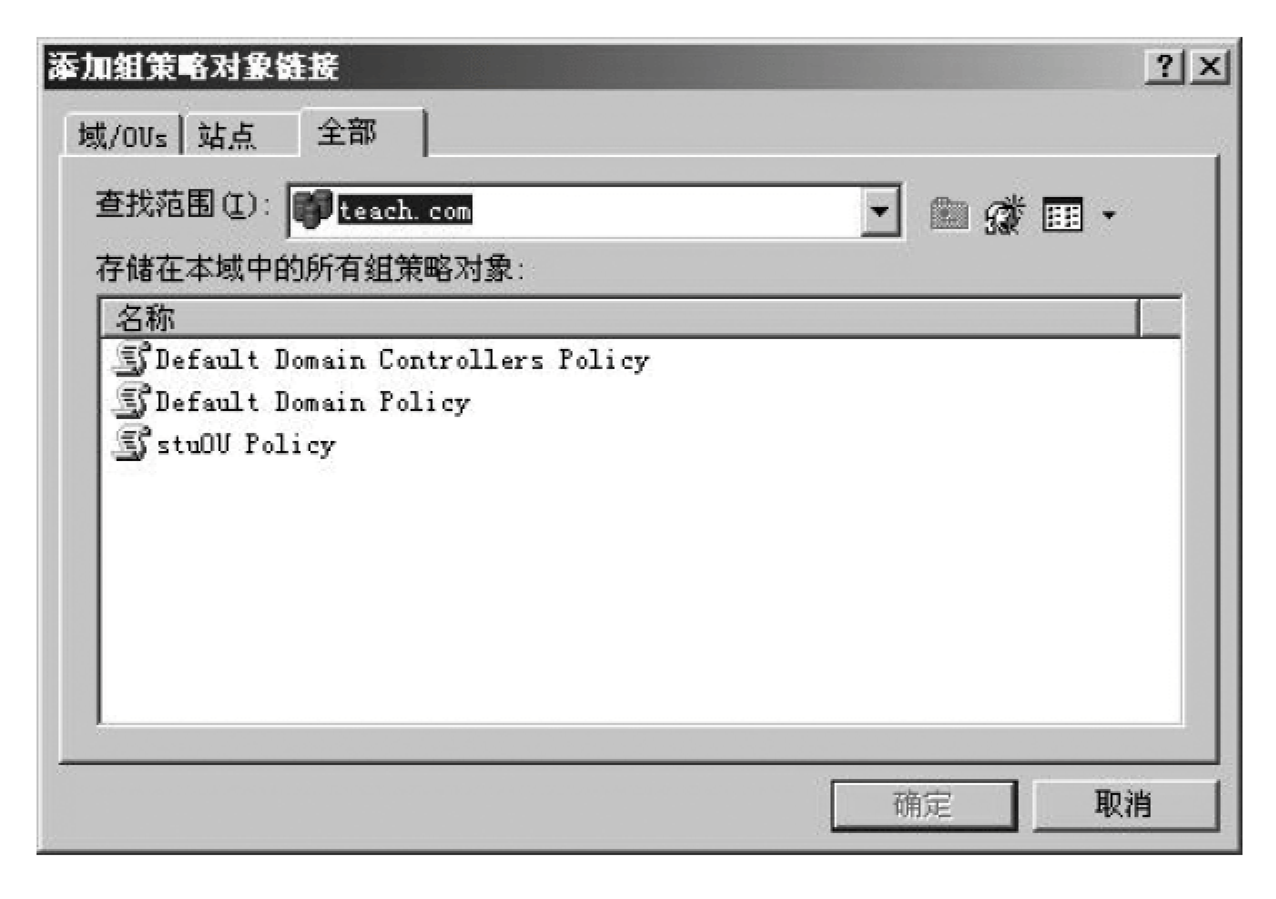


图 9-95 【添加组策略对象链接】对话框的【全部】选项卡



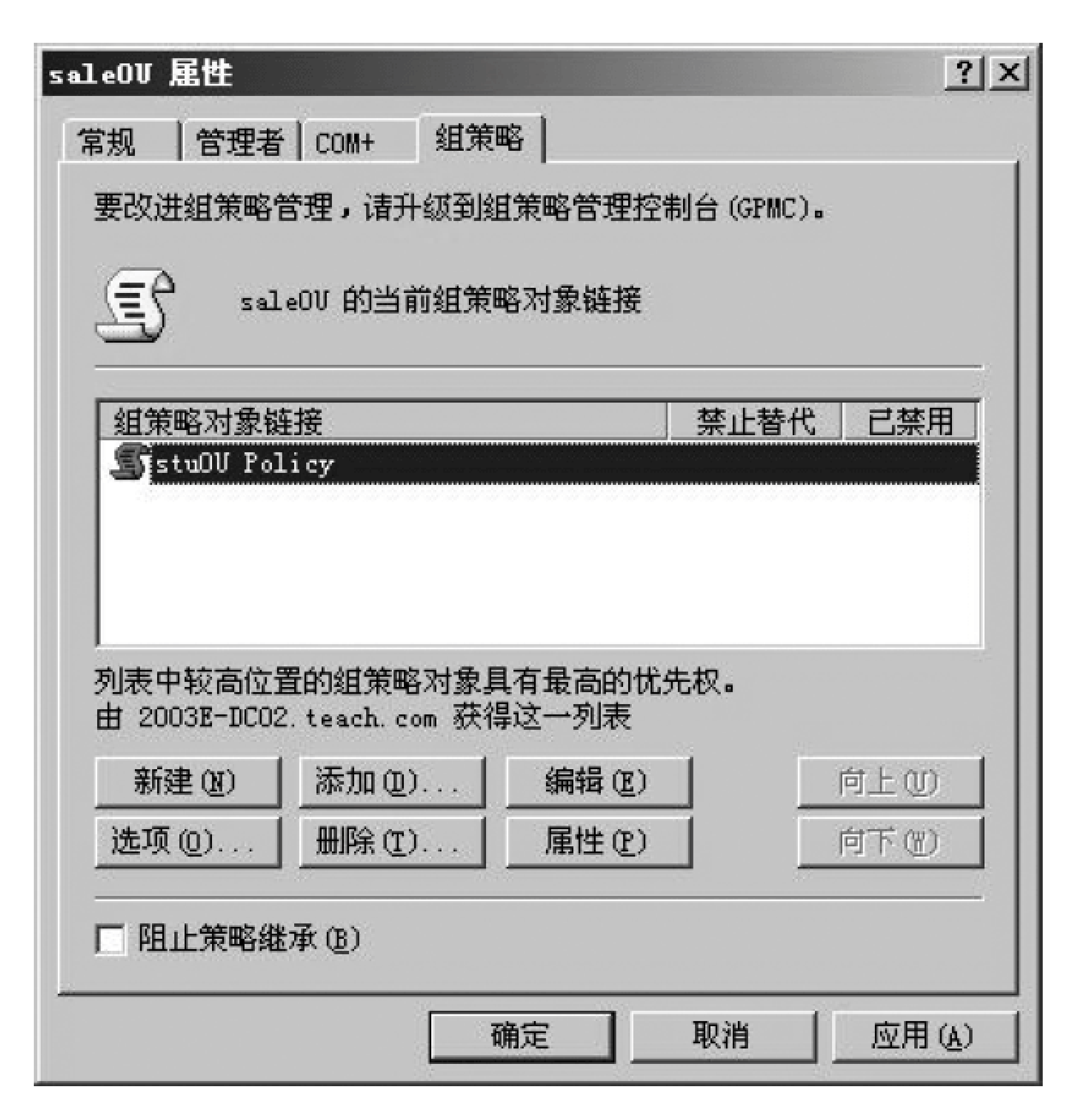


图 9-96　添加 GPO 链接后的【saleOU 属性】对话框

9.10.5　删除 GPO 链接

删除 GPO 链接就是将 GPO 与指定的站点、域或 OU 之间的链接断开。GPO 仍然保留在 AD 中，直至被删除。删除 GPO 链接的步骤如下：

(1) 参考前面的步骤，打开【Active Directory 用户和计算机】窗口，在左侧窗口中选择想要断开链接的站点、域或 OU(如 saleOU)，右击，在弹出的快捷菜单中选择【属性】命令，打开【saleOU 属性】对话框的【组策略】选项卡(图 9-96)。

(2) 在【组策略对象链接】列表中选择选择需要删除的 GPO(如 stuOU Policy)，单击【删除】按钮。弹出【删除】对话框(图 9-97)，选择【从列表中移除链接】单选按钮，单击【确定】按钮。



图 9-97　【删除】对话框

(3) 返回【saleOU 属性】对话框，可以看到 stuOU Policy 组策略被删除了。单击【关闭】按钮完成设置。

(4) 运行 gpupdate 命令，刷新组策略。

提示：参考 9.10.4 小节的步骤，重新打开如图 9-95 所示的对话框，可以看到在【存储在本域中的所有组策略对象】列表中，stuOU Policy 组策略对象仍然存在。说明上述操作只是删除了 stuOU Policy 组策略对象与 saleOU 组织单位的链接，GPO 仍然保留在 AD 中。



9.10.6 删除 GPO

如果删除 GPO,即从 AD 中将其删除,那么该 GPO 所链接的任何站点、域或组织单位都不会再受到它的影响。删除 GPO 有以下两种方法。

方法一：参考 9.10.5 小节的步骤,只需在如图 9-97 所示的对话框中选择【移除链接并将组策略对象永久删除】单选按钮即可。

方法二：参考 9.10.4 小节的步骤,在如图 9-95 所示的对话框中选择要删除的 GPO(如 stuOU Policy),右击,选择【删除】命令(图 9-98),弹出【删除组策略对象】对话框(图 9-99)。单击【是】按钮,返回如图 9-95 所示的对话框,可以看到 stuOU Policy 已被删除(图 9-100)。



图 9-98 利用【添加组策略对象链接】对话框删除 GPO

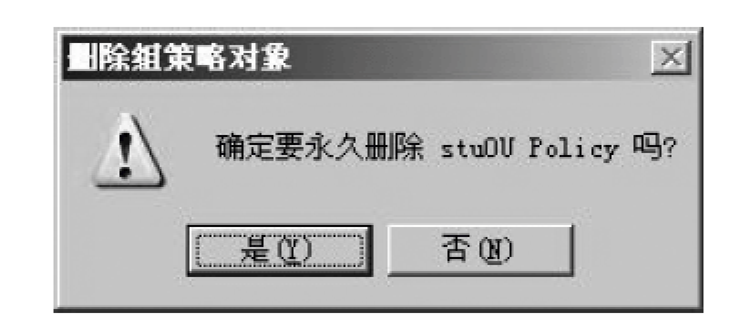


图 9-99 【删除组策略对象】对话框

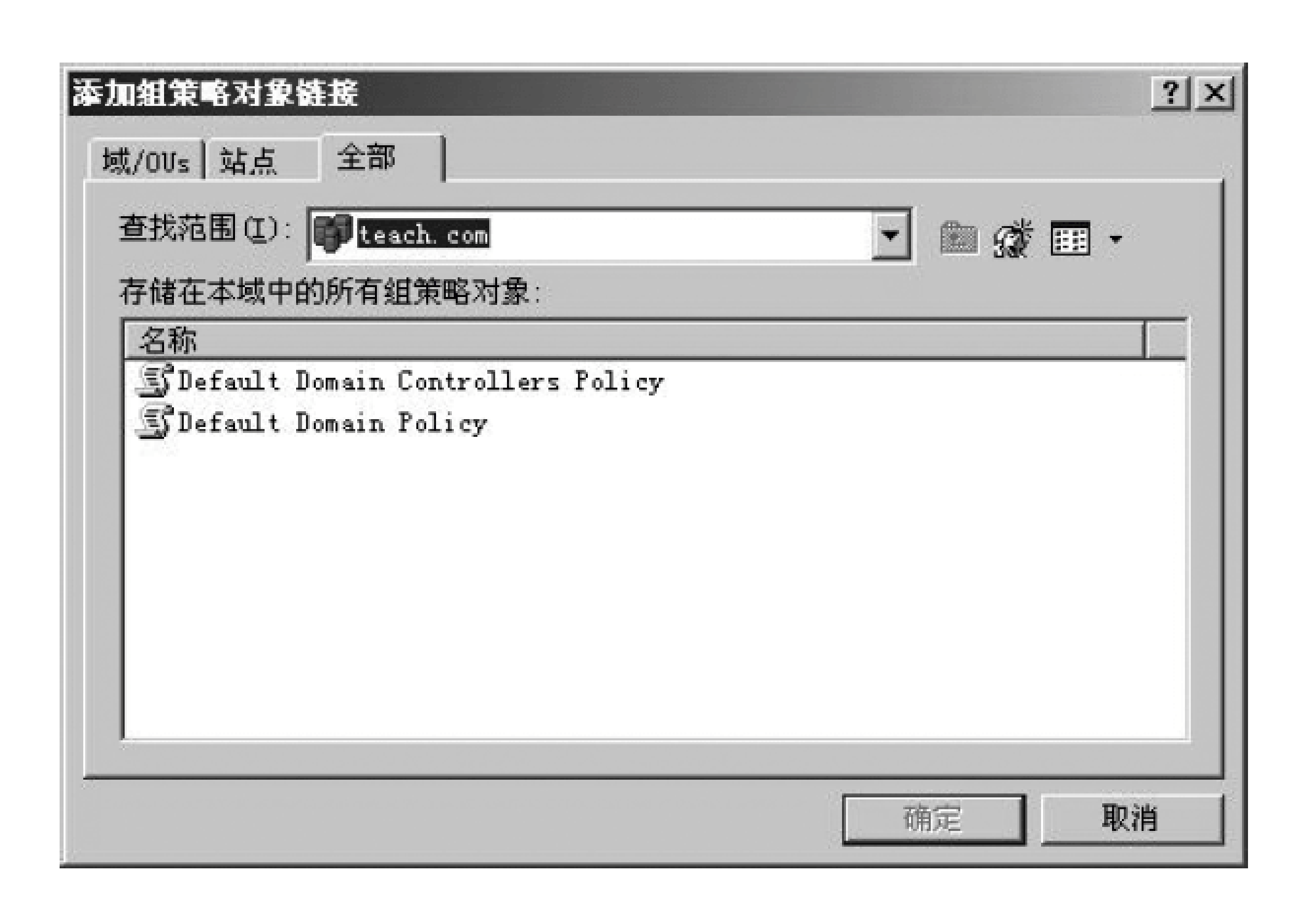


图 9-100 删除 GPO 后的【添加组策略对象链接】对话框

注意：如果要删除的 GPO 已经与所有站点、域或组织单位无链接,那么只有采取方法二才能将其从 AD 中删除。





9.11　组策略应用规则

组策略应用规则包括如下五个方面：继承与阻止继承、强制生效、累加、应用顺序和筛选。

9.11.1　继承与阻止继承

1. 继承

默认情况下，下层容器会继承来自上层容器的 GPO。

例如，在 stuOU 组织单位中创建名为 studeOU 的子 OU，并将 stu002 账户移动到该子 OU 中。在 stuOU 组织单位中添加创建名为 stuOU-2 Policy 的 GPO，设置 IE 主页 URL 为 http://www.lzzy.net，那么无论是 stuOU 中的 stu001 账户，还是 studeOU 中的 stu002 账户，登录客户机后，IE 主页地址都为：http://www.lzzy.net。详细操作步骤如下：

（1）以 Administrator 账户登录域控制器，参考 9.10.3 小节的步骤，创建 studeOU 子容器，并将 stu002 账户移动到该子 OU 中。

（2）参考 9.10.3 小节的步骤，在 stuOU 组织单位中添加创建名为 stuOU-2 Policy 的 GPO（图 9-101），单击【编辑】按钮，打开【组策略编辑器】对话框。



图 9-101　【stuOU 属性】对话框

（3）在左侧窗口的目录树中，选择【用户配置】/【Windows 设置】/【Internet Explorer 维护】/【URL】选项（图 9-102）。

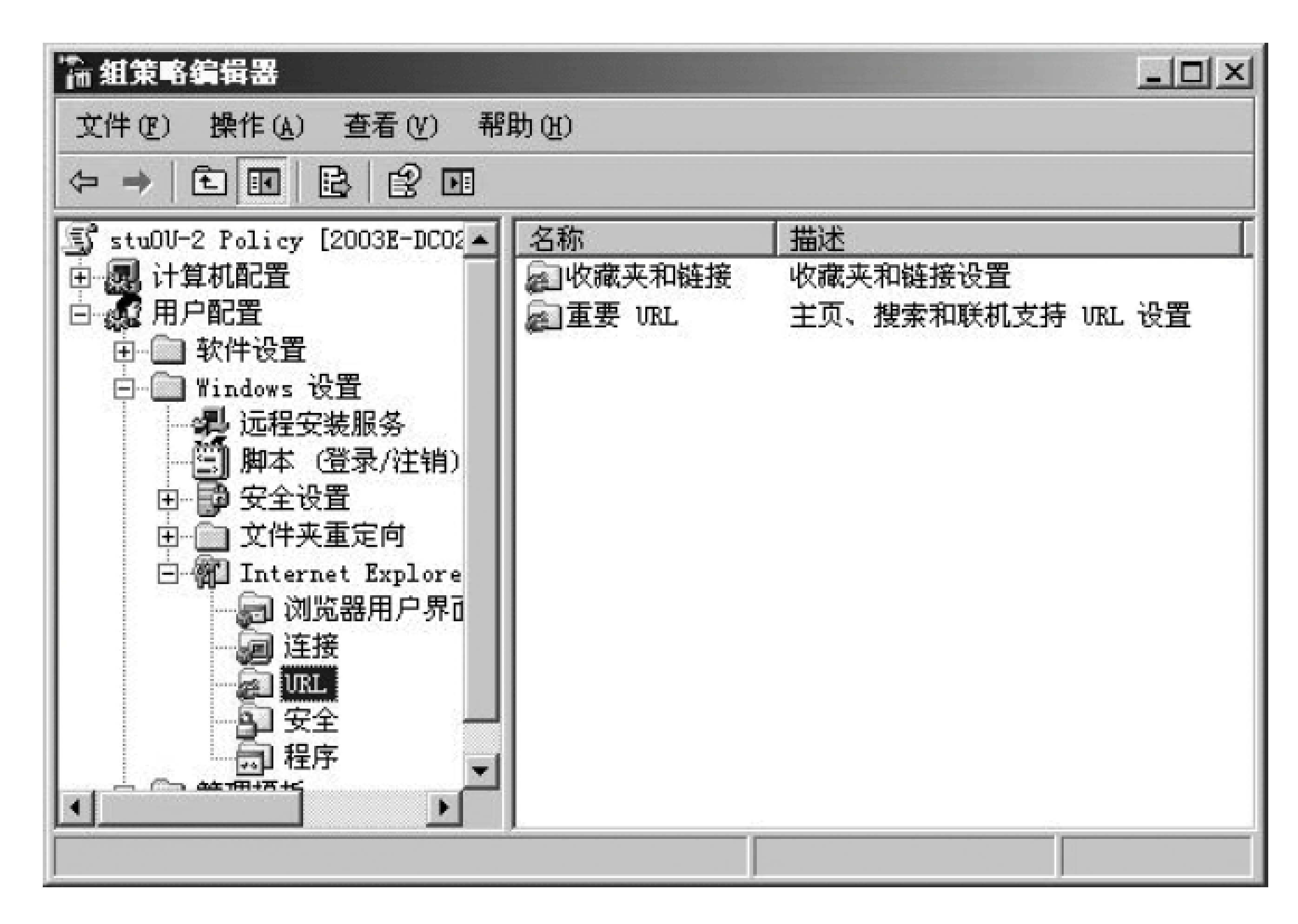


图 9-102　【Internet Explorer 维护】/【URL】选项



(4) 双击右侧详细信息列表窗格中的【重要 URL】选项，打开【重要 URL】对话框，选中【自定义主页】复选框，在【主页 URL】文本框中输入：http://www.lzzy.net(图 9-103)。关闭所有对话框。

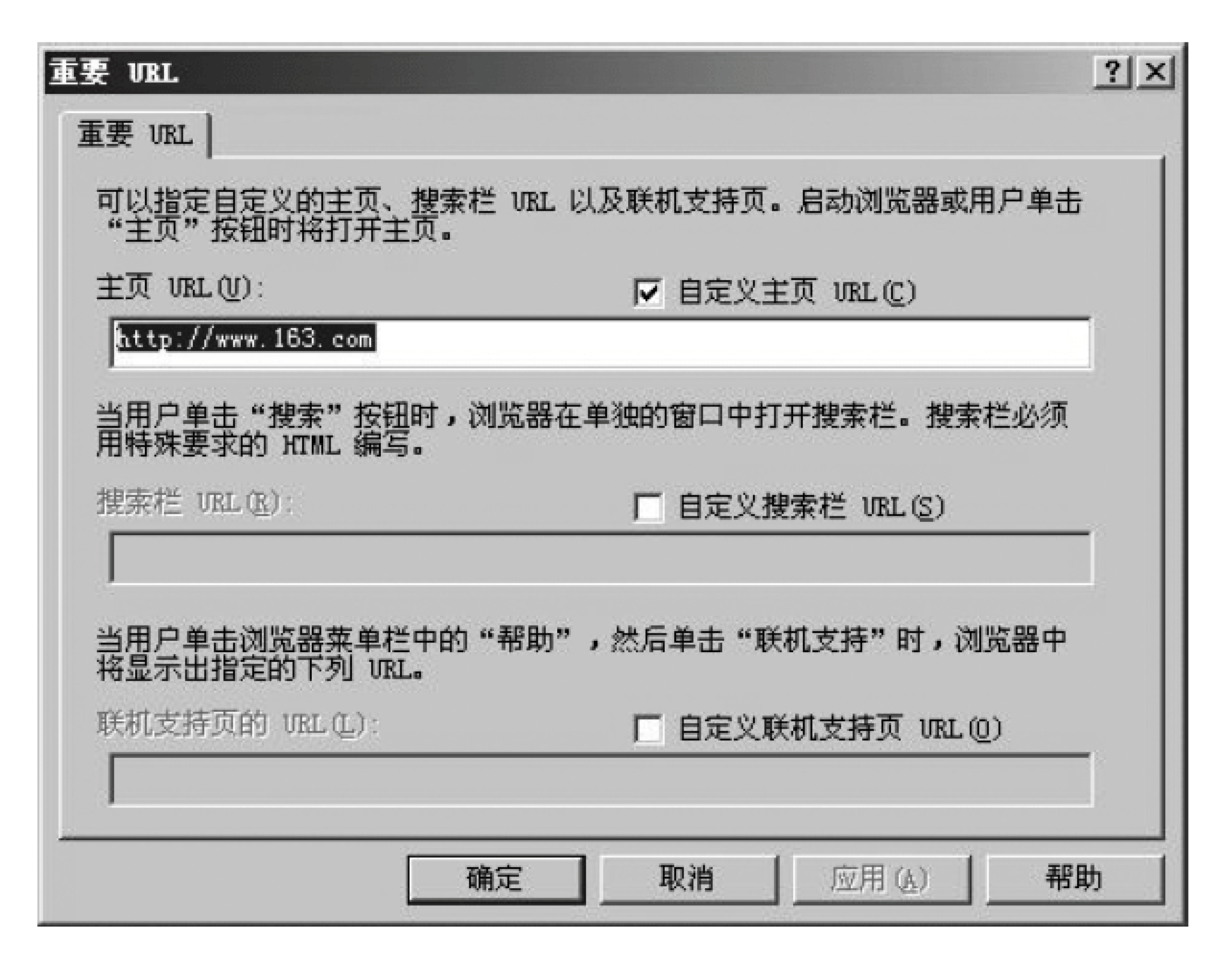


图 9-103 【重要 URL】对话框

(5) 运行 gpupdate 命令，刷新组策略。

(6) 验证。以 stu002 账户登录客户端，打开 IE 浏览器，可以看到默认打开的主页为：http://www.lzzy.net。

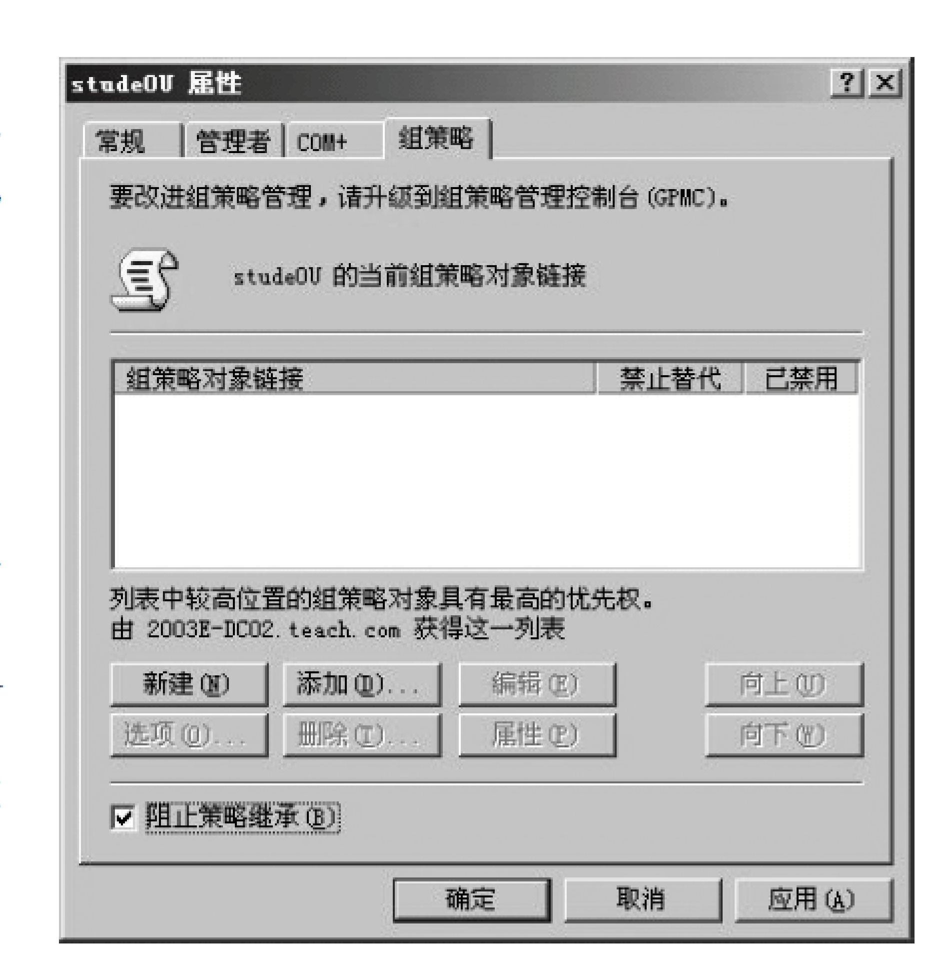


图 9-104 【studeOU 属性】对话框的【组策略】选项卡

2. 阻止继承

子容器可以阻止上级的组策略。例如要阻止 studeOU 子 OU 继承上级的组策略，则步骤如下：

(1) 参考 9.10.3 小节的步骤，打开【studeOU 属性】对话框的【组策略】选项卡，选中【阻止策略继承】复选框(图 9-104)，单击【确定】按钮即可。

(2) 运行 gpupdate 命令，刷新策略。

组策略继承与阻止继承规则实例设置及结果如表 9-10 所示。

表 9-10 继承与阻止继承规则实例设置及结果

stuOU 的 GPO 设置	是否继承	StudeOU 子 OU 的有效设置
stuOU-2 Policy 设置为：IE 主页 URL 为 http://www.lzzy.net	继承	IE 主页 URL 为 http://www.lzzy.net
	阻止继承	IE 主页 URL 不为 http://www.lzzy.net

9.11.2 强制生效

强制生效是上级容器强制下级容器执行其 GPO 设置。



例如强制 studeOU 子 OU 继承上级的 stuOU-2 Policy 组策略。详细步骤如下：

（1）参考 9.11.1 小节的步骤，打开如图 9-101 所示的【stuOU 属性】对话框，单击【选项】按钮，打开【stuOU-2 Policy 选项】对话框，选中【禁止替代】复选框（图 9-105）。

（2）单击【确定】按钮，返回【stuOU 属性】对话框，可以看到【组策略对象链接】列表中的【禁止替代】选项被选中（如图 9-106）。



图 9-105　【stuOU-2 Policy 选项】对话框

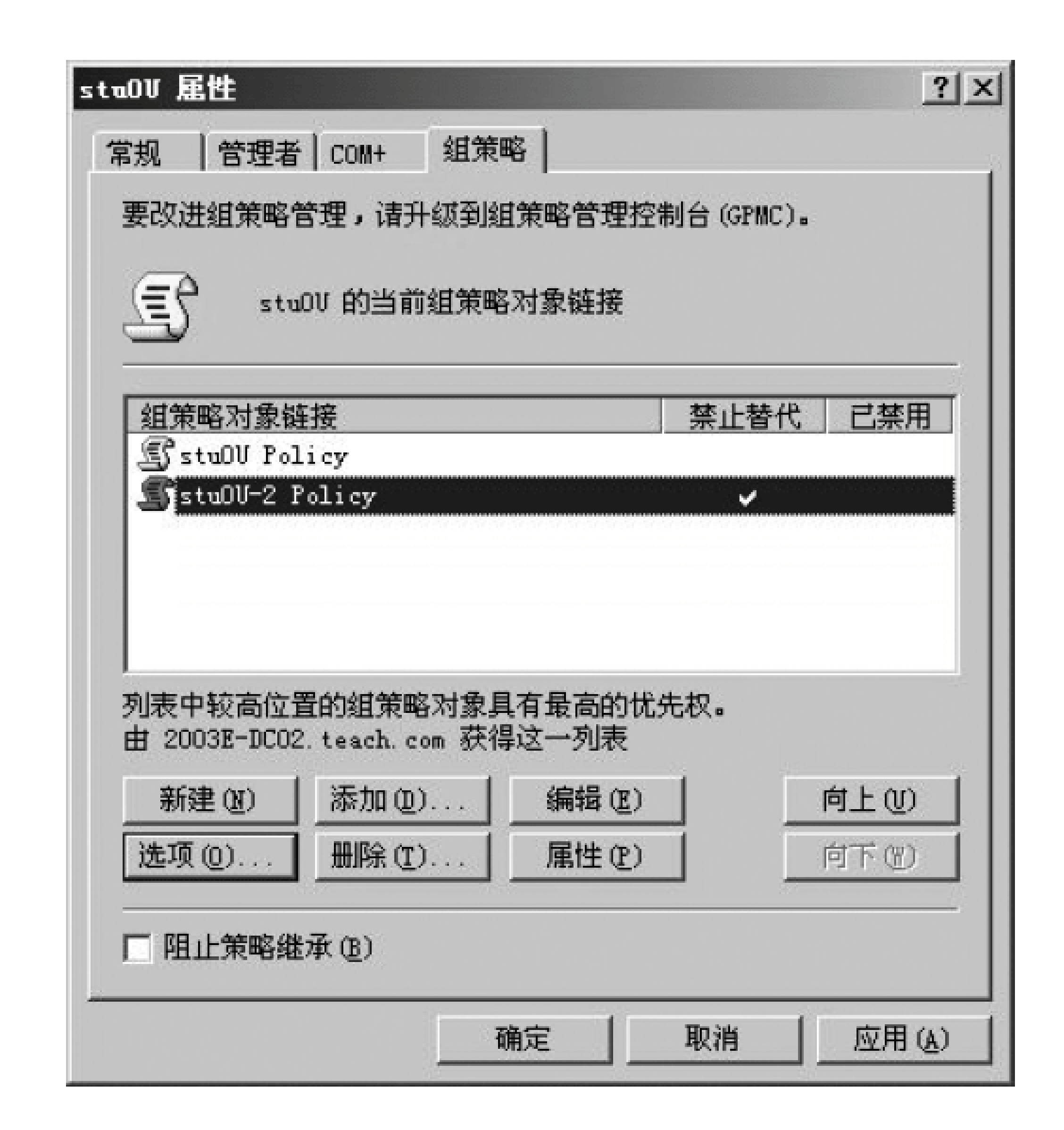


图 9-106　【stuOU 属性】对话框

（3）运行 gpupdate 命令，刷新策略。

（4）验证。以 stu002 账户登录客户端，打开 IE 浏览器，可以看到默认打开的主页为 http://www.lzzy.net，即子 OU 被强制继承上级组策略。

9.11.3　累加

容器的多个组策略设置如果不冲突，则最终的有效策略是所有组策略设置的总和；容器的多个组策略设置如果冲突，则后应用的组策略覆盖先应用的组策略。

例如，stuOU 组织单位的 stuOU Policy 组策略设置了禁止用户更改桌面墙纸，该 OU 的 stuOU-2 组策略设置了 IE 主页 URL。以 stu001 账户登录客户端，可验证有效策略是所有组策略设置的总和。

如果修改 stuOU Policy 组策略，设置 IE 主页为：http://jpkc.lzzy.net/网络安全技术.html，并刷新组策略。在客户端上注销 stu001 账户，再以该账户重新登录，打开 IE 浏览器，可以看到默认打开的主页为 http://jpkc.lzzy.net/网络安全技术.html。验证了如果多个组策略设置冲突，则后应用的组策略覆盖先应用的组策略。

组策略累加规则实例设置及结果如表 9-11 所示。



表 9-11　策略累加规则实例设置及结果

stuOU 的 GPO 设置		是否冲突	stuOU 的有效设置
第 1 次	stuOU Policy 设置为：已启用“阻止更改墙纸”	否	启用“阻止更改墙纸”
	stuOU-2 Policy 设置为：IE 主页 URL 为 http://www.lzzy.net		IE 主页 URL 为 http://www.lzzy.net
第 2 次	stuOU Policy 设置(不变)	是	禁用“阻止更改墙纸”
	stuOU-2 Policy 设置为：已禁用“阻止更改墙纸”		

9.11.4　应用顺序

GPO 用于存储组策略的配置信息，用于控制对站点、域和 OU 中的计算机及用户的设置。在 Windows Server 2003 中有本地组策略、域组策略、域控制器组策略和 OU 组策略。它们的应用顺序如图 9-107所示(优先级由低到高)。

例如，在 studeOU 子 OU 中创建名为 studeOU Policy 的 GPO，设置启用“禁止用户访问控制面板”。在 stuOU 中编辑 stuOU-2 Policy 组策略，设置禁用“禁止用户访问控制面板”。按如下步骤操作并验证策略的应用顺序。

(1) 参考 9.10.3 小节的步骤，在 studeOU 组织单位中添加创建名为 studeOU Policy 的 GPO(图 9-108)，单击【编辑】按钮，打开【组策略编辑器】窗口。

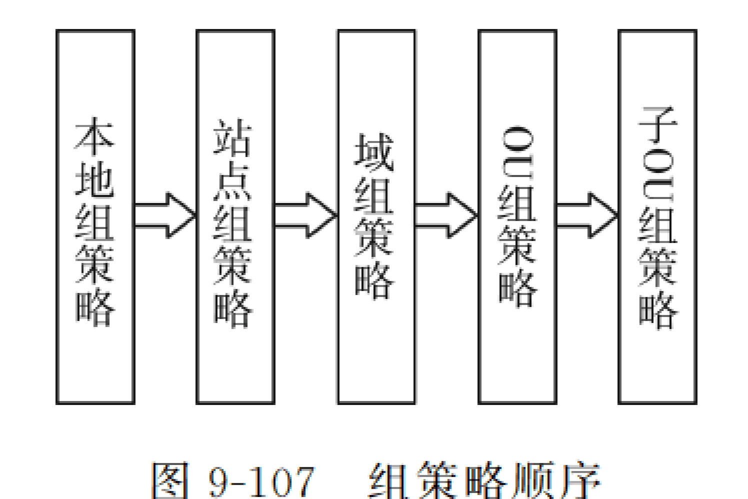


图 9-107　组策略顺序

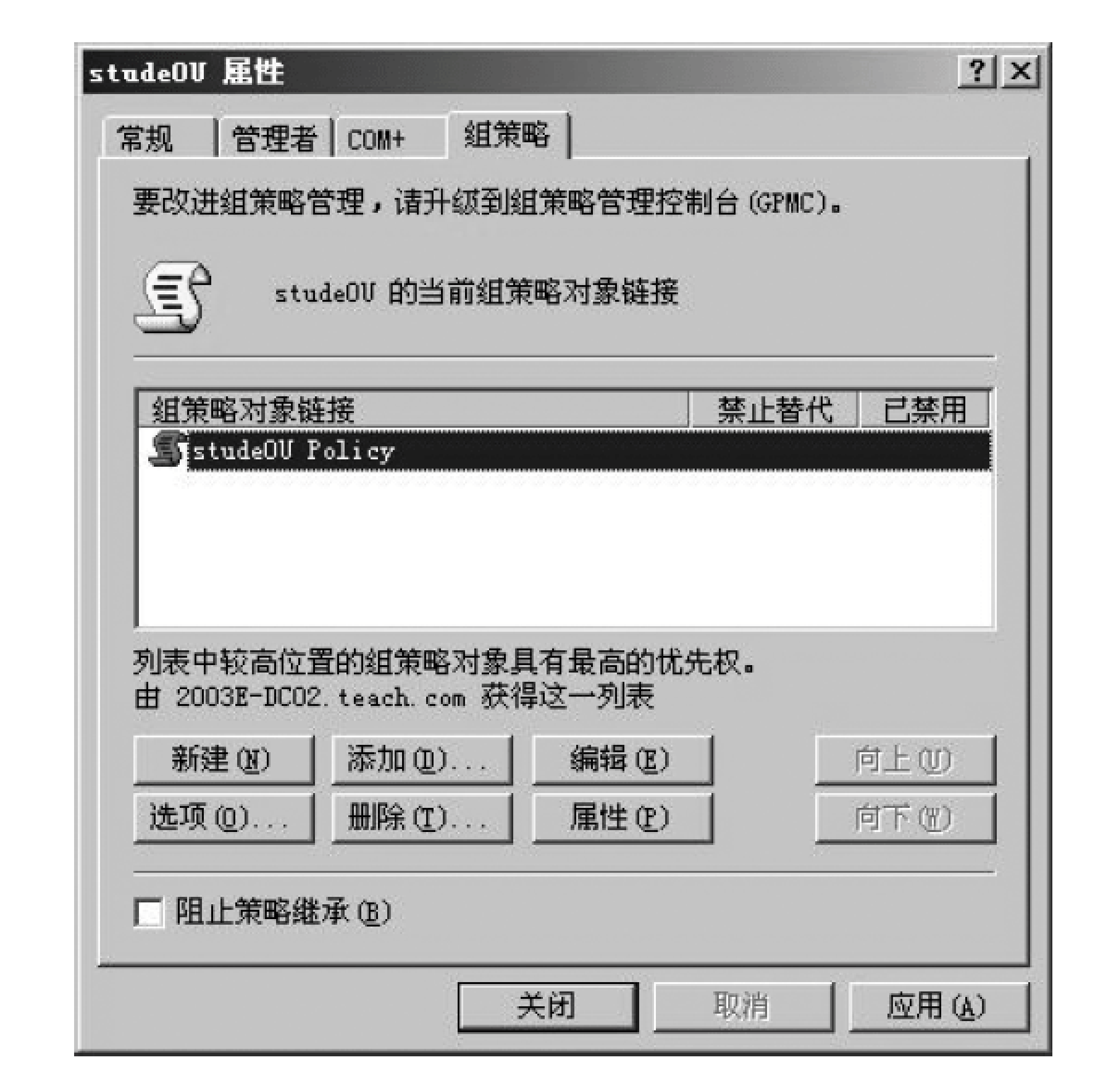


图 9-108　【studeOU 属性】对话框

(2) 在左侧窗口的目录树中，选择【用户配置】/【管理模板】/【控制面板】选项(图 9-109)。

(3) 双击右侧详细信息列表窗格中的【禁止访问控制面板程序】选项，打开【禁止访问控





图 9-109　【用户配置】/【管理模板】/【控制面板】选项

制面板 属性】对话框，选择【已启用】单选按钮(图 9-110)，单击【确定】按钮，关闭所有对话框。



图 9-110　【禁止访问控制面板 属性】对话框

(4) 参考上述方法，在 stuOU 组织单位中，设置 stuOU-2 Policy 的 GPO 为：已禁用“禁止访问控制面板”。

(5) 运行 gpupdate 命令，刷新组策略。

(6) 验证。以 stu002 账户登录客户端，尝试访问控制面板失败。说明子 OU 的应用顺序高于 OU 的应用顺序。

组策略应用顺序实例设置及结果如表 9-12 所示。



表 9-12　组策略应用顺序实例设置及结果

组策略设置	是否冲突	StudeOU 子 OU 的有效设置
先设置子 OU 组策略，studeOU Policy 设置为：已启用“禁止用户访问控制面板”	是	启用“禁止用户访问控制面板”
后设置 OU 组策略，stuOU-2 Policy 设置为：已禁用“禁止用户访问控制面板”		

9.11.5　筛选

筛选可以阻止一个 GPO 应用于容器内的特定计算机和用户。

例如，在 teach.com 域中创建名为 teach Policy 的 GPO，设置启用“禁止用户访问控制面板”，并要求 info 组的用户账户除外。详细操作步骤如下：

(1) 参考 9.10.3 小节的步骤，在 teach.com 域中添加创建名为 teach Policy 的 GPO（图 9-111）。参考 9.11.4 小节的步骤，在该 GPO 中设置启用“禁止用户访问控制面板”。

(2) 返回如图 9-111 所示的对话框后，单击【属性】按钮，在打开的【teach Policy 属性】对话框中选择【安全】选项卡（图 9-112）。



图 9-111　【teach.com 属性】对话框的【组策略】选项卡



图 9-112　【teach Policy 属性】对话框的【安全】选项卡(一)

(3) 单击【添加】按钮，参考 9.6.2 小节的步骤，选择 info 组，返回上级对话框，确认在【组或用户名称】列表中选择 info 组，然后在【info 的权限】列表中选中【应用组策略】选项的【拒绝】复选框（图 9-113），单击【确定】按钮，关闭所有对话框。

(4) 运行 gpupdate 命令，刷新组策略。

(5) 验证。以 info 组的 info002 账户登录客户端，尝试打开控制面板，如果成功，说明通过筛选设置，阻止了 teach.com 域的策略应用于 info 组的所有用户。



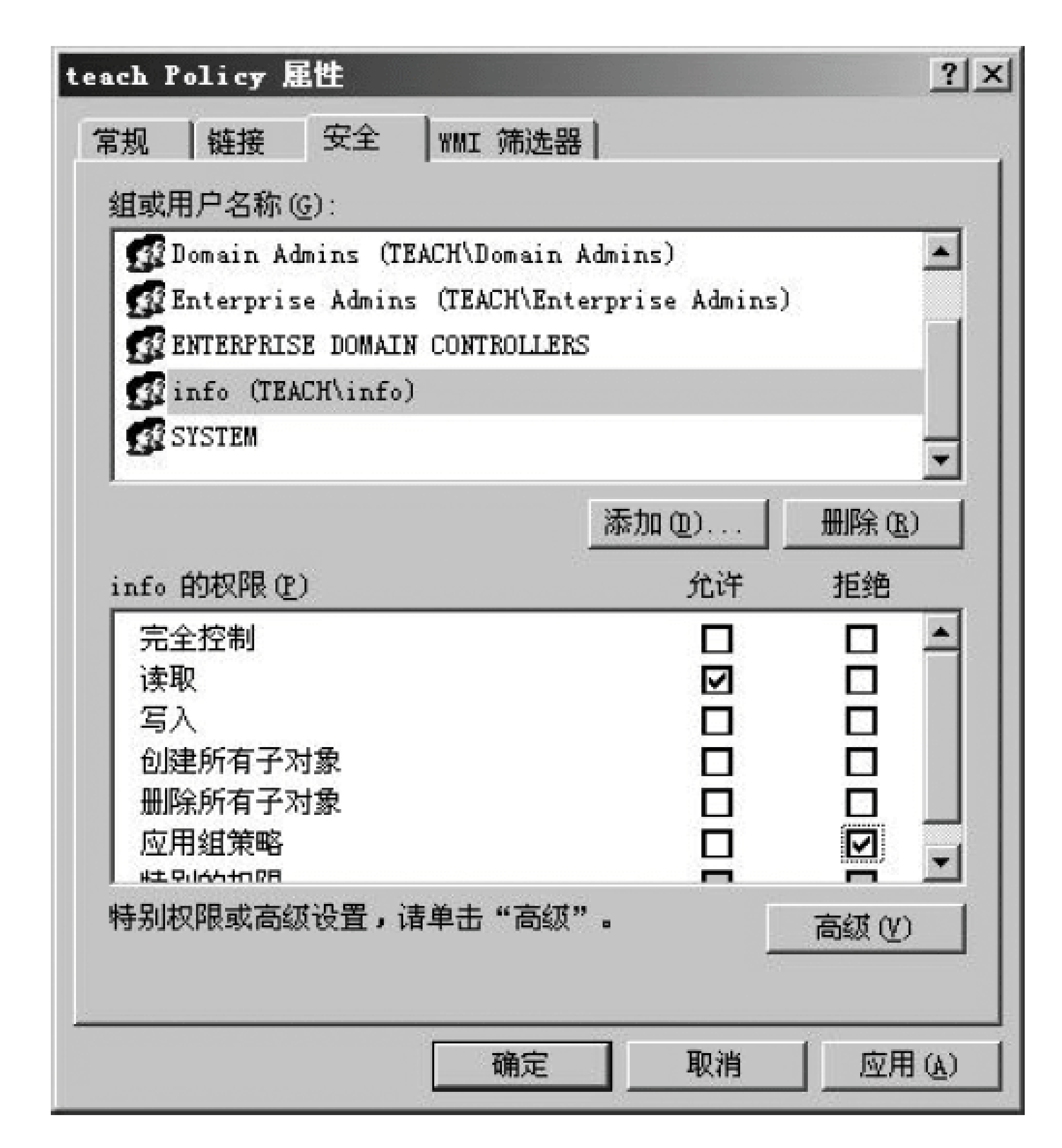


图 9-113　【teach Policy 属性】对话框的【安全】选项卡(二)

9.12　利用组策略限制软件的执行

9.12.1　软件限制策略概述

软件限制策略旨在满足控制未知或不信任的软件的需求。随着网络、Internet 以及电子邮件在商务计算方面的使用日益增多，用户发现他们经常会遇到新软件。用户必须不断作出是否该运行未知软件的决定。病毒和特洛伊木马经常故意地伪装自己以骗得用户的运行。要用户做出安全的选择来确定应运行的程序是非常困难的。

使用软件限制策略，可通过标志并指定允许运行的软件来保护计算机环境免受不信任软件的侵袭。可以为 GPO 定义“不受限的”或“不允许的”的默认安全级别，从而决定是否在默认情况下允许软件运行。通过为特定软件创建软件限制策略规则，可以对默认安全级别作出例外安排。例如，如果将默认的安全级别设为“不允许的”，则可以创建允许运行特定的软件的规则。

使用软件限制策略可以实现以下目的。

(1) 控制软件在系统中的运行能力。例如，担心用户在电子邮件中收到病毒，可以应用策略设置不允许某些文件类型在电子邮件程序的附件目录中运行。

(2) 允许用户在多用户计算机上仅运行特定文件。例如，在计算机上有多个用户，可以设置软件限制策略：除用户工作所需的特定文件外，他们不能访问任何软件。

(3) 决定可以在计算机中添加信任的发布者的用户。

(4) 控制软件限制策略是作用于所有用户，还是仅作用于计算机上的某些用户。

(5) 阻止任何文件在本地计算机、组织单位、站点或域中运行。例如，系统中存在已知病毒，则使用软件限制策略阻止计算机打开含有这些病毒的文件。



利用组策略限制软件执行的方法有两种：利用【不要运行指定的 Windows 应用程序】选项和利用【软件限制策略】选项。

9.12.2　利用【不要运行指定的 Windows 应用程序】选项限制软件的执行

利用【不要运行指定的 Windows 应用程序】选项限制软件的步骤如下：

（1）以 Administrator 账户登录域控制器，参考前面的步骤，在 stuOU 组织单位中创建名为“限制软件执行”的 GPO（图 9-114）。单击【编辑】按钮，打开【组策略编辑器】窗口。

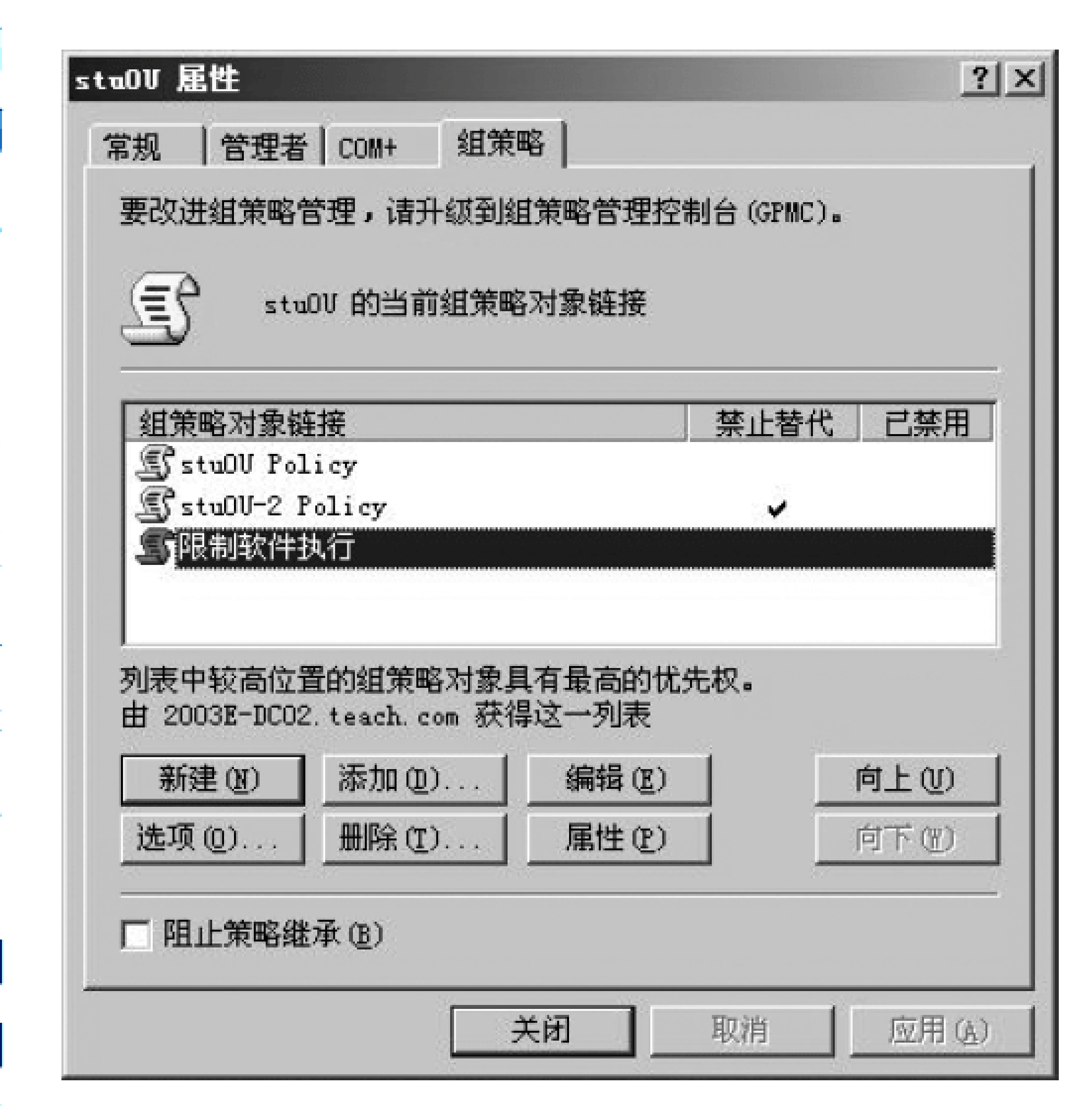


图 9-114　【stuOU 属性】对话框

（2）在左侧窗口的目录树中，选择【用户配置】/【管理模板】/【系统】选项，在右侧详细信息列表窗格中选择【不要运行指定的 Windows 应用程序】选项（图 9-115），双击，打开【不要运行指定的 Windows 应用程序 属性】对话框，选择【已启用】单选按钮（图 9-116）。

（3）单击【显示】按钮，打开【显示内容】对话框。单击【添加】按钮，在【添加项目】对话框中输入需要限制执行的文件名。例如禁止 stuOU 组织单位中所有用户执行 QQ2009，而该软件的执行文件为 QQ.exe。那么就输入 QQ.exe（图 9-117），单击【确定】按钮，返回上级对话框，可以看到“QQ.exe”出现在【不允许的应用程序的列表】列表框中（图 9-118）。



图 9-115　【组策略编辑器】窗口





图 9-116 【不要运行指定的 Windows 应用程序 属性】对话框

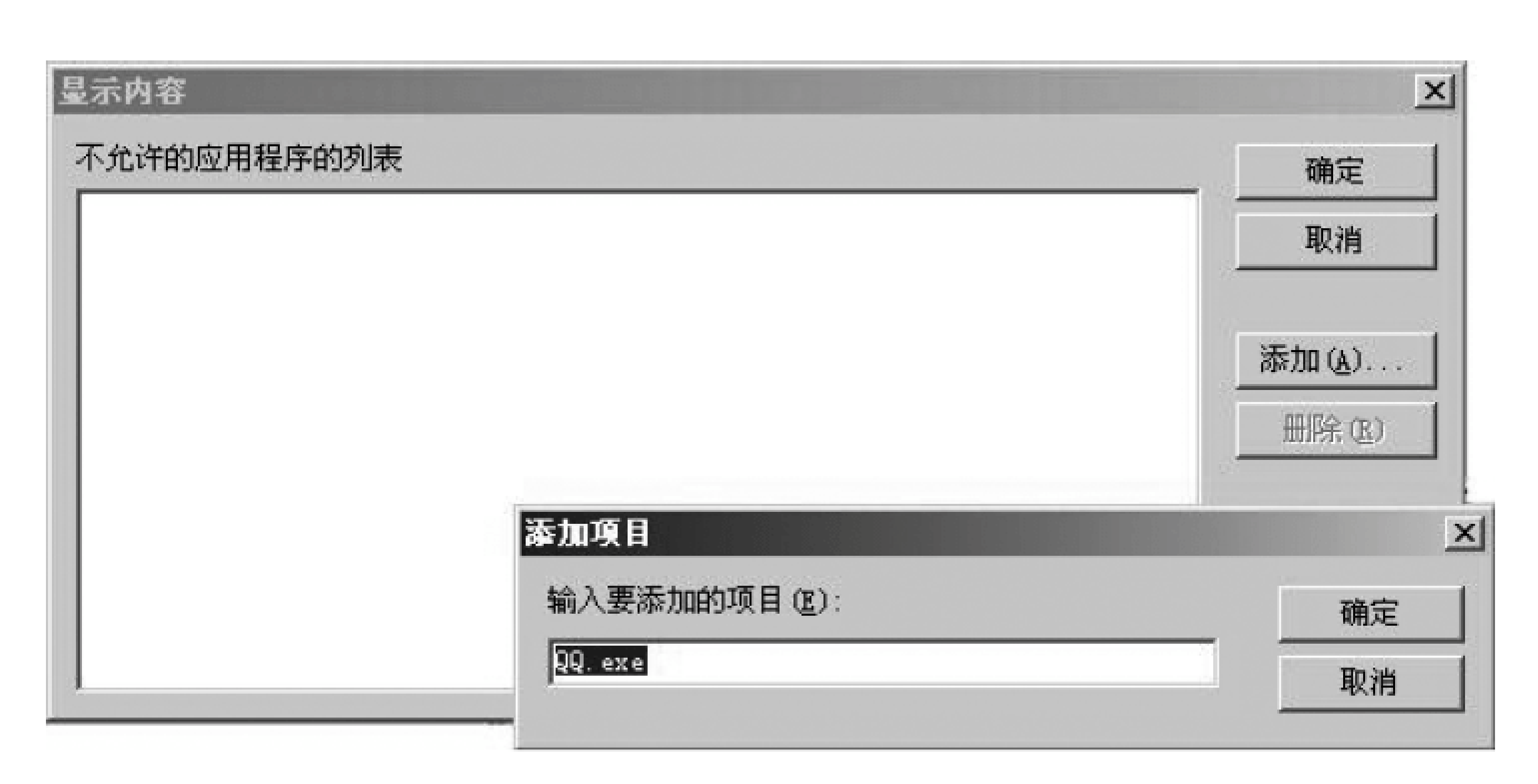


图 9-117 【添加项目】对话框

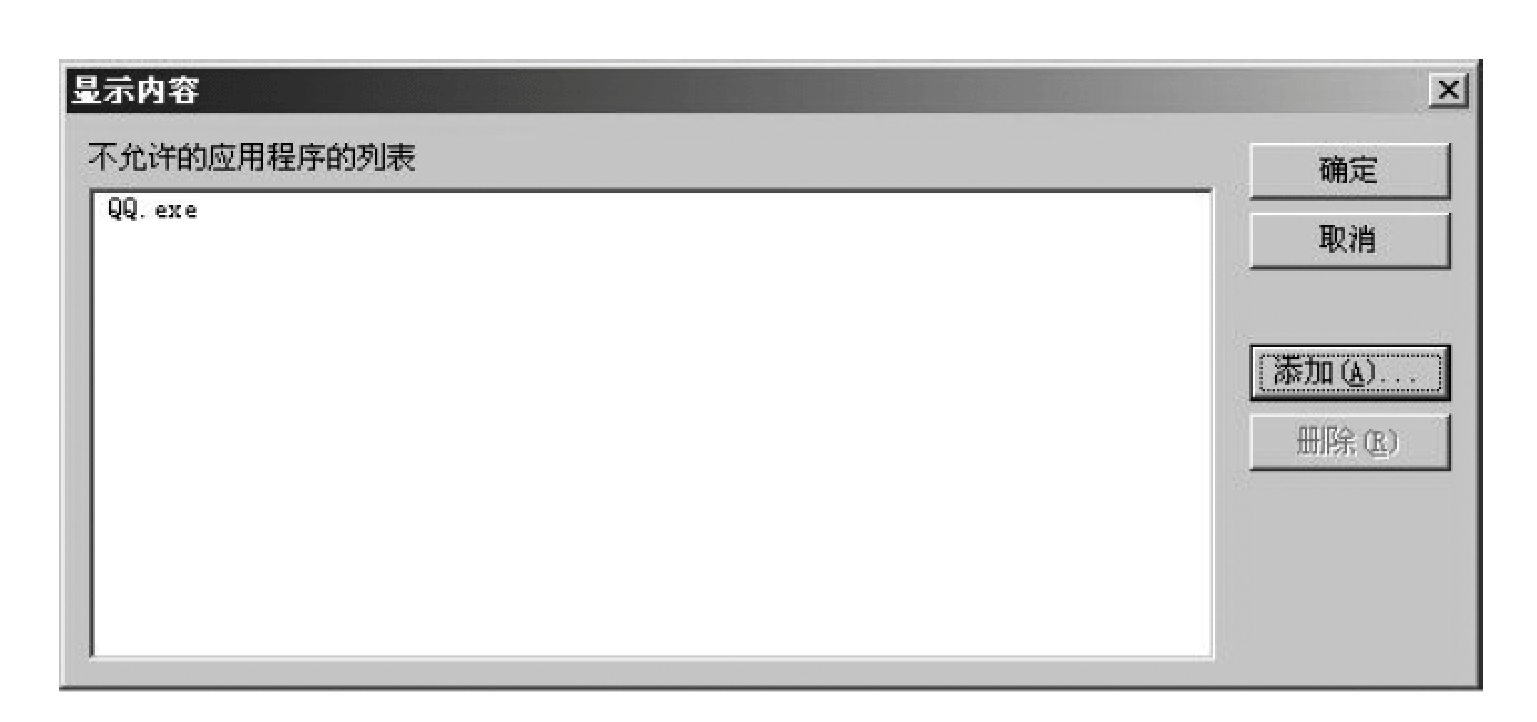


图 9-118 “QQ. exe”出现在【不允许的应用程序的列表】列表框中

(4) 单击【确定】按钮,返回上级对话框。再次单击【确定】按钮,返回【stuOU 属性】对话框,单击【关闭】按钮即可。

(5) 运行 gpupdate 命令,刷新组策略。

(6) 以 stu002 账户登录客户端,尝试执行 QQ. exe 文件,弹出【限制】对话框(图 9-119),提示操作被限制。



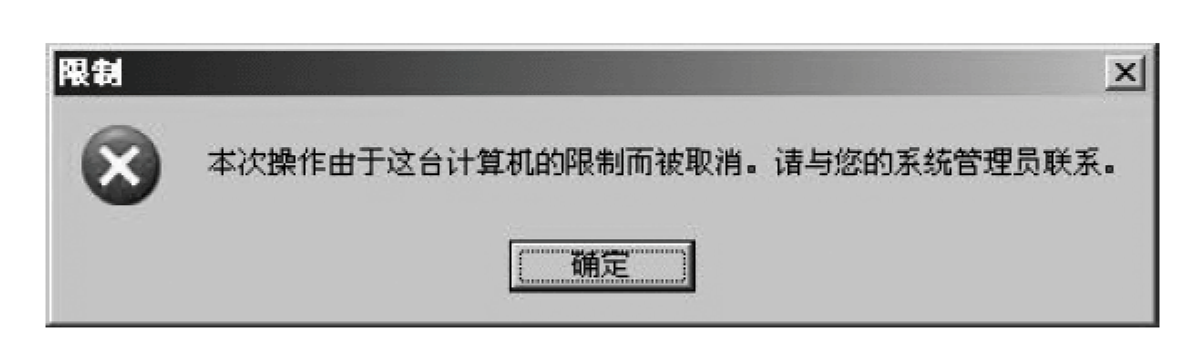


图 9-119 【限制】对话框

此方法存在不足之处：如果用户改变程序的文件名，例如将 QQ.exe 改变 QQ2009.exe，则可以避开此策略的限制了。为了防止这种情况，必须采用下面介绍的另一种方法。

9.12.3 利用【软件限制策略】选项限制软件的执行

系统默认的安全等级是所有软件都没有限制，即只要用户对想执行的软件拥有适当的访问权限就能执行它。但可以通过四种规则建立例外的安全等级，以便限制用户执行所指定的软件，这些规则包括哈希规则、证书规则、路径规则和 Internet 区域规则等。利用【软件限制策略】选项限制软件的执行需要用到哈希规则，因此在此只介绍哈希规则。

哈希(hash)是根据软件程序(文件)的内容计算出来的一串字节，不同的软件必定有不同的哈希值，因此可以用此值来辨别不同的软件。

为某个软件建立哈希规则后，系统会为该软件计算出其哈希值。当用户执行此软件时，用户的计算机会自动重新计算其哈希值，对比该哈希值与软件限制中的哈希值，如果相同，则拒绝此软件执行。即使用户改变软件的名称或移动到别的地方，该软件的哈希值都不会改变，因此该软件都会在该策略影响范围内受到限制。

下面说明如何利用哈希规则来禁止 stuOU 组织单位中所有用户执行 QQ2009。详细步骤如下：

(1) 以 Administrator 账户登录域控制器，参考 9.12.2 小节的步骤，打开如图 9-115 所示窗口。选择【用户配置】/【Windows 设置】/【安全设置】/【软件限制策略】选项，在其上右击，在弹出的快捷菜单中选择【创建软件限制策略】命令(图 9-120)。

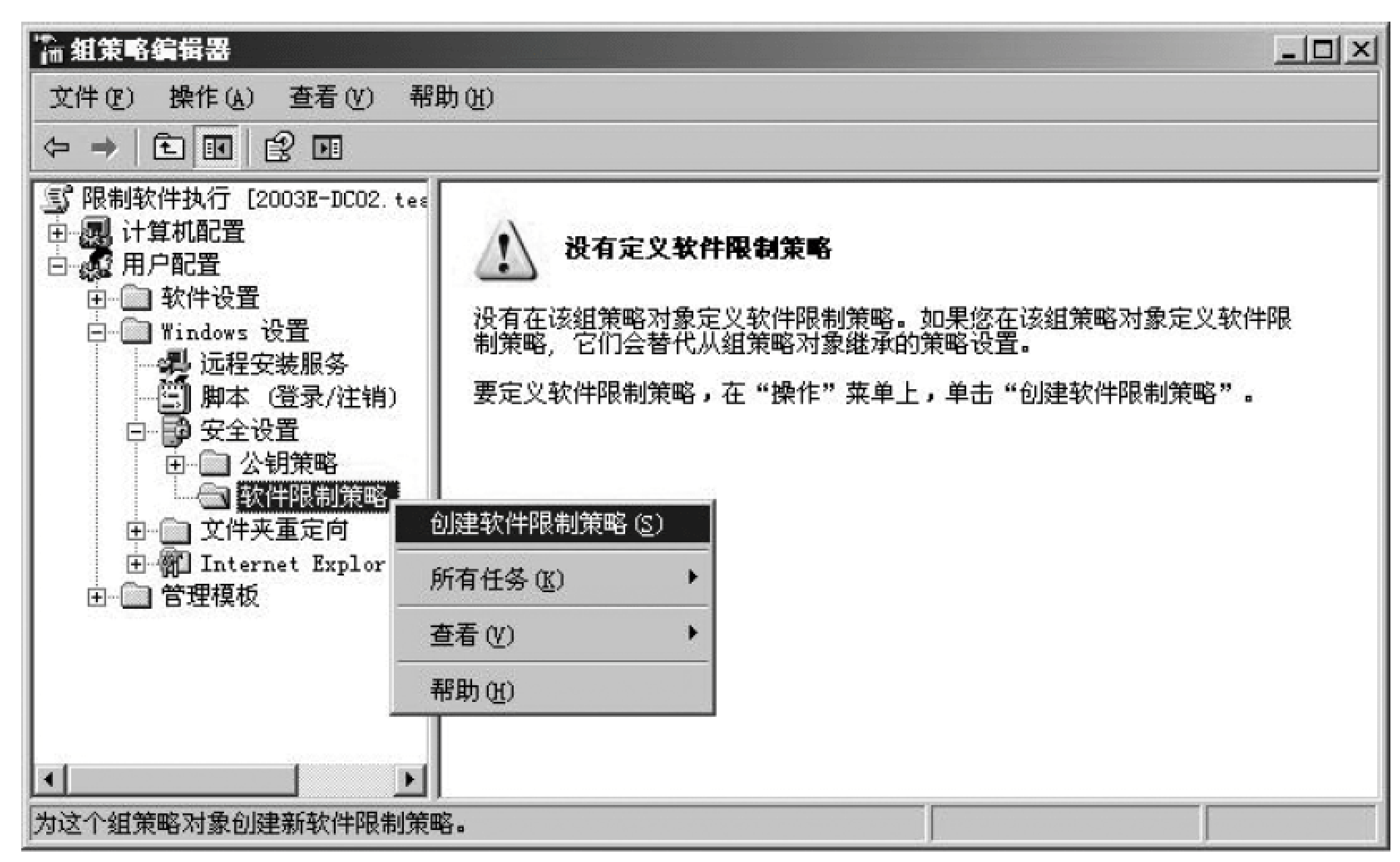


图 9-120 选择【创建软件限制策略】命令



(2) 在右侧详细信息列表窗格(或左侧窗口目录树中)的【其他规则】选项上右击，在弹出的快捷菜单中选择【新建哈希规则】命令(图 9-121)，打开【新建哈希规则】对话框(图 9-122)。



图 9-121 选择【新建哈希规则】命令

(3) 单击【浏览】按钮，找到 QQ2009 的执行文件 QQ.exe 并选择，单击【打开】按钮确定。然后系统进行哈希值的运算，运算完成后，返回【新建哈希规则】对话框，可以看到运算后的文件的哈希值及文件信息(图 9-123)。

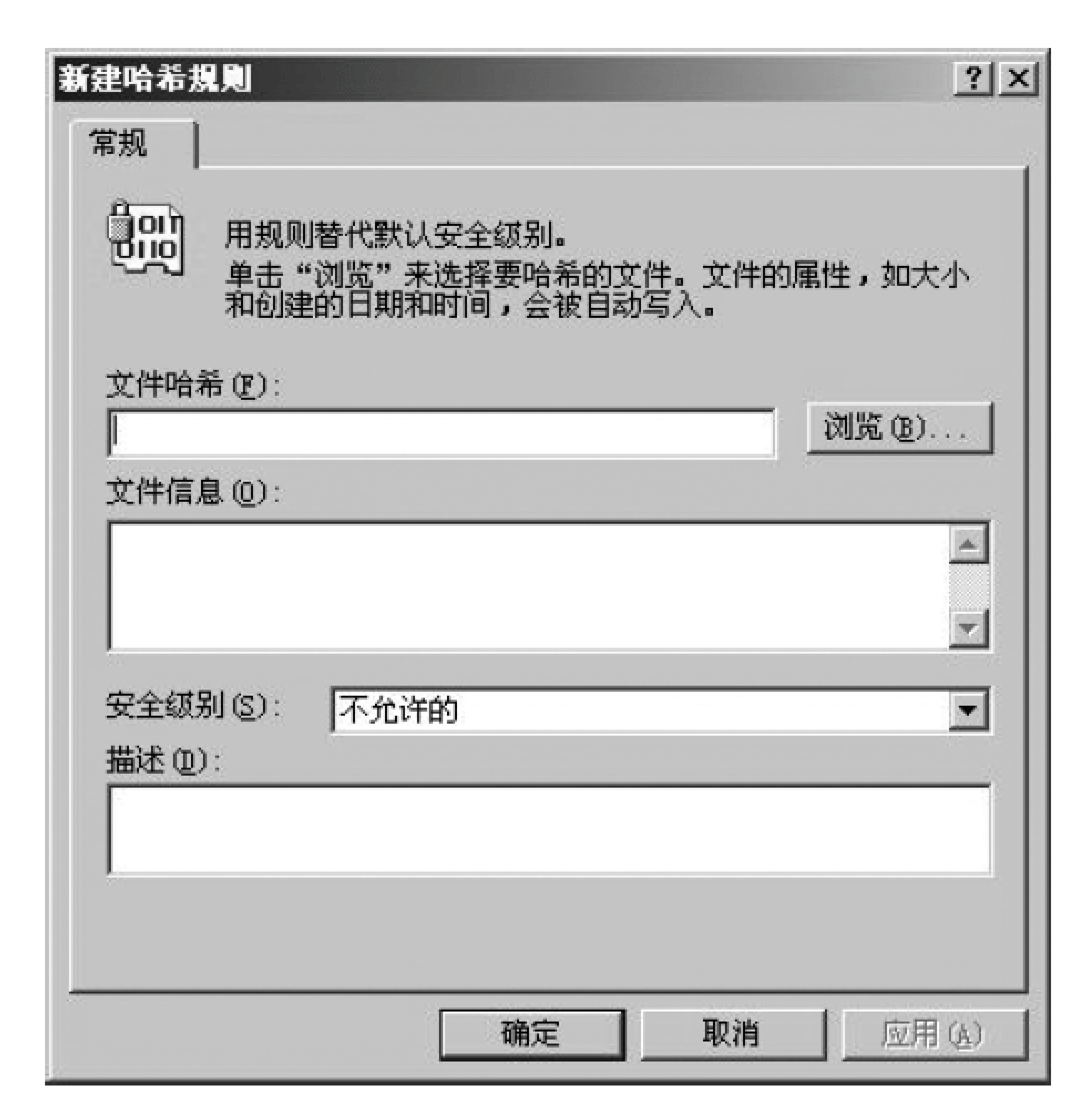


图 9-122 【新建哈希规则】对话框

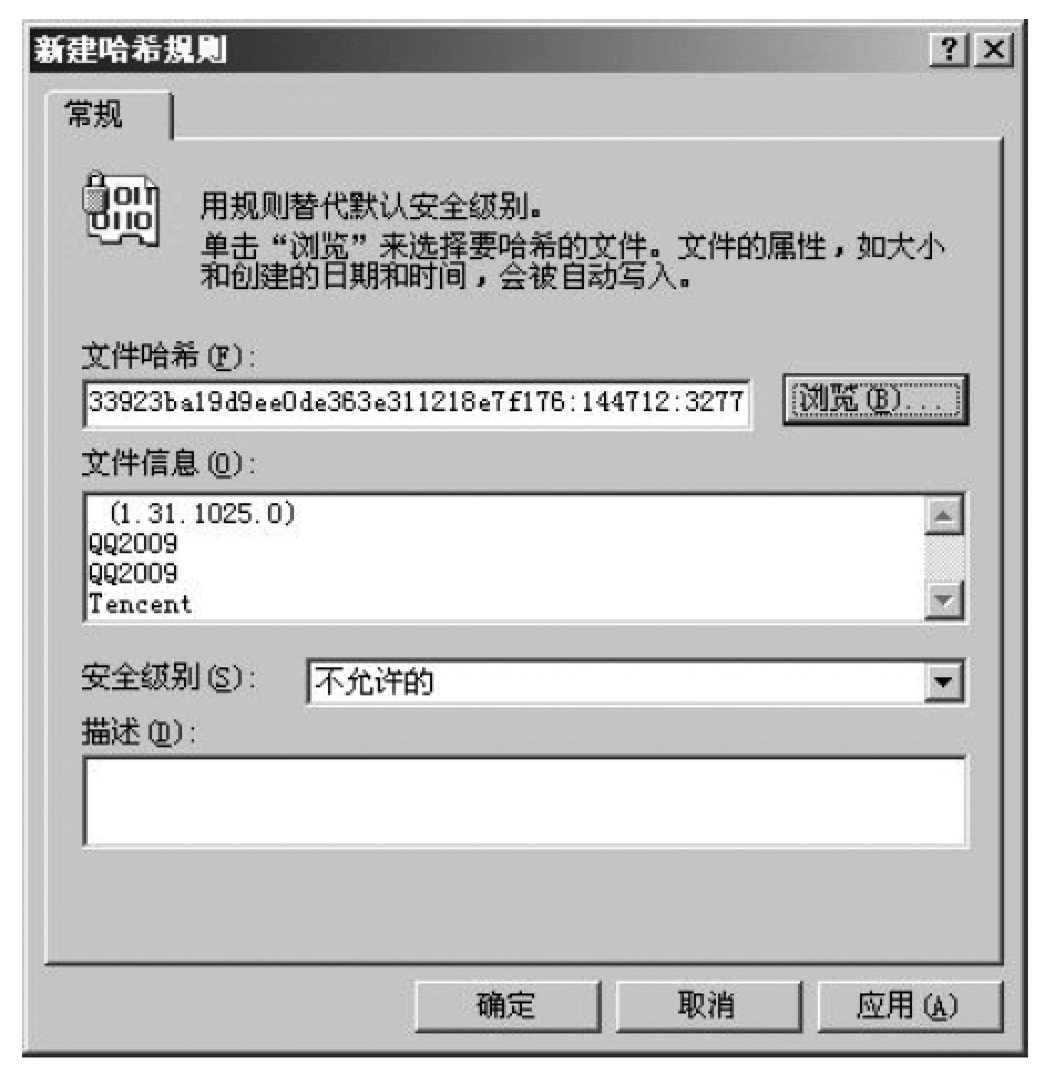


图 9-123 运算后的文件的哈希值及文件信息

(4) 确认图中【安全级别】选项值为【不允许的】后，单击【确定】按钮。

(5) 返回【组策略编辑器】窗口，双击打开右侧详细信息列表窗格中的【其他规则】选项，可以看到 QQ2009 被限制的显示(图 9-124)。



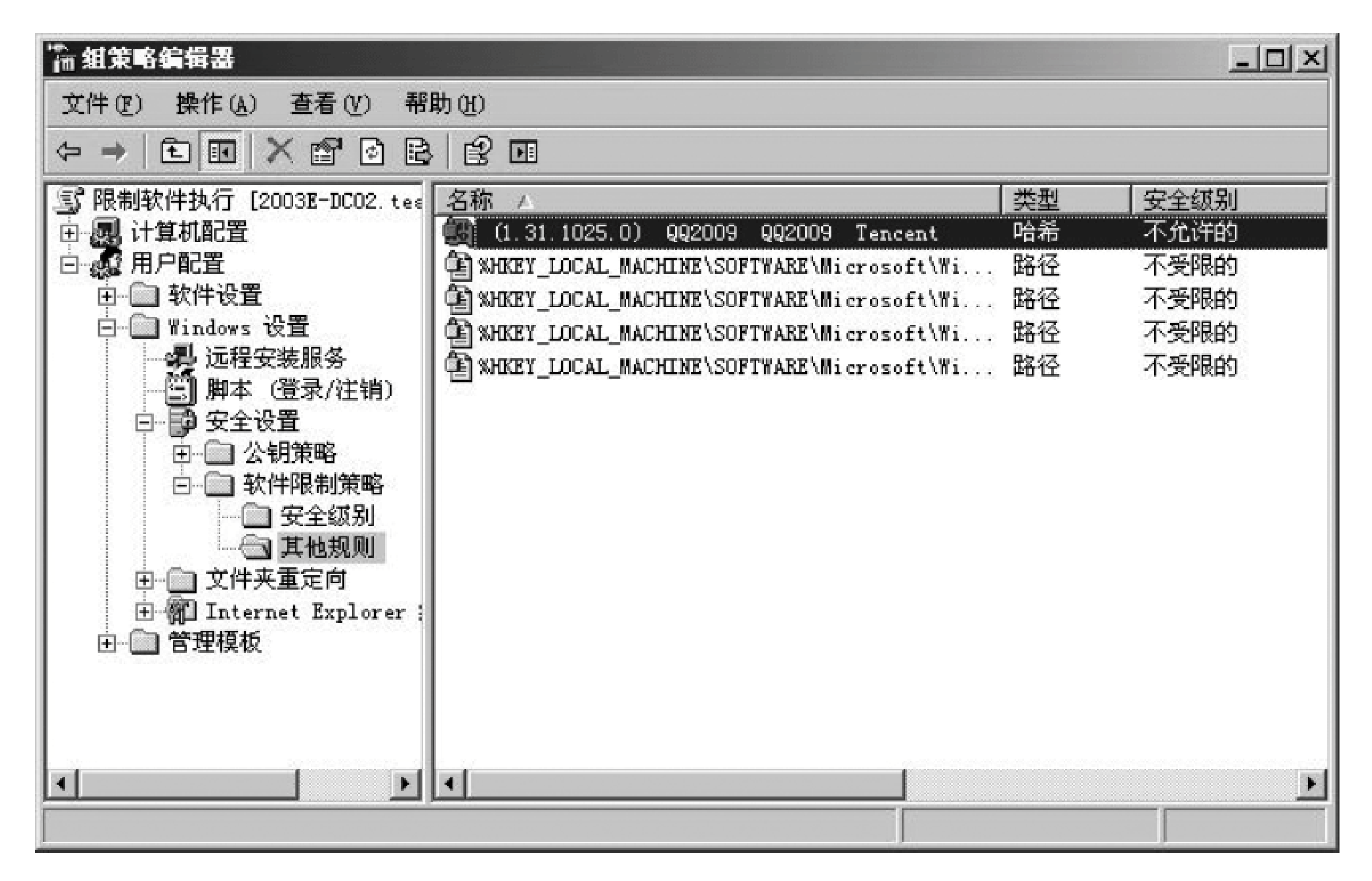


图 9-124 【组策略编辑器】窗口中的【其他规则】选项

(6) 运行 gpupdate 命令,刷新组策略。

(7) 在客户端注销 stu002 账户,并以该账户重新登录,将 QQ.exe 文件改名为 QQ2009.exe 后,尝试执行,结果弹出【限制】对话框(图 9-119),提示操作被限制。

注意: 如果将 9.12.1 小节的方法停用,再验证 9.12.2 小节的方法,则弹出的警告画面将如图 9-125 所示。

C:\Program Files\Tencent\QQ\Bin\QQ.exe

C:\Program Files\Tencent\QQ\Bin\QQ.exe

由于一个软件限制策略的阻止,Windows 无法打开此程序。要获取更多信息,请打开事件查看器或与系统管理员联系。

确定

图 9-125 警告对话框

9.13 习 题

1. 简述 NTFS 权限规则。
2. NTFS 权限设置包括哪些内容?
3. 举例说明 AGDLP 规则的应用。
4. 简述本地安全策略的内容。
5. 简述域控制器安全策略与本地安全策略的区别。
6. 简述本地安全策略、域控制器安全策略与域安全策略三者之间的关系,并举例说明它们的应用。
7. 简述组策略的作用及其应用规则。
8. 如何利用组策略实现限制软件的执行?





第10章　系统安全风险评估

本章学习目标：

- 风险评估的国际标准。
- 各种风险评估分析方法的适用场合。
- 风险评估的具体实施步骤。

在当今信息时代，基于网络的威胁潜伏在每一个角落。对一个黑客而言，闯入一个计算机系统从来就不是绝对不可能的，只是困难程度不同而已。病毒、恶意代码、木马、人为破坏、自然物理故障等给信息系统带来了巨大的威胁，为了防止和降低这些安全风险，业界投入了大量的人力、物力寻求解决方法。前面介绍的防火墙技术、防病毒技术、入侵检测系统、漏洞扫描技术、加密、安全认证等技术推陈出新，但是却没有从根本上解决信息系统的安全局限。

安全是一个动态的过程，不能通过一次技术的组合就解决全部安全问题。安全风险评估通过合理的分析方法，检测信息系统存在的安全隐患，并制定有效的安全措施，以防止对系统安全构成威胁的事件发生。信息安全风险评估是一个不断降低安全风险的过程，其最终目的是使安全风险降低到一个可接受的程度，使用户和决策者可以接受剩余的风险。

10.1　风险评估概述

10.1.1　概述

风险（Risk）指在某一特定环境下，在某一特定时间段内，特定的威胁利用资产的一种或一组薄弱点，导致资产的丢失或损害的潜在可能性。网络安全的缺陷及用户对安全策略的遵守不利经常会导致基于 Internet 的攻击者更方便地对网络进行定位并危及其安全。

风险评估（Risk Assessment）指组织使用适当的风险评估工具，对信息和信息处理设施的威胁（Threat）、影响（Impact）和脆弱性（Frangibility）及其发生的可能性的评估，也就是确认安全风险及其大小的过程。风险评估是任何一个试图正确管理系统安全的组织所应该进行的第一个步骤，它为安全管理的后续工作提供方向和依据，后续工作的优先等级和关注程度都是由信息安全风险决定的。

风险评估的目的，就是使信息系统的使用者对于其管理的信息系统有一个全面的认识，



对于其中的安全问题、安全建设思路有深刻的认识。通过风险评估,暴露信息系统面临的各种威胁,通过评估这些威胁出现的概率,确定它们可能给系统带来的损失。通过风险评估可以帮助我们制定有效的安全解决方案,提高系统的安全状况。

10.1.2 风险评估的风险模型

目前国内主流的信息安全厂商例如中联绿盟信息技术(北京)有限公司、启明星辰信息技术有限公司、联想、华为、安络科技等,都几乎一致地采用了类似的概念和风险评估的模型。其基本原理图如图 10-1 所示。

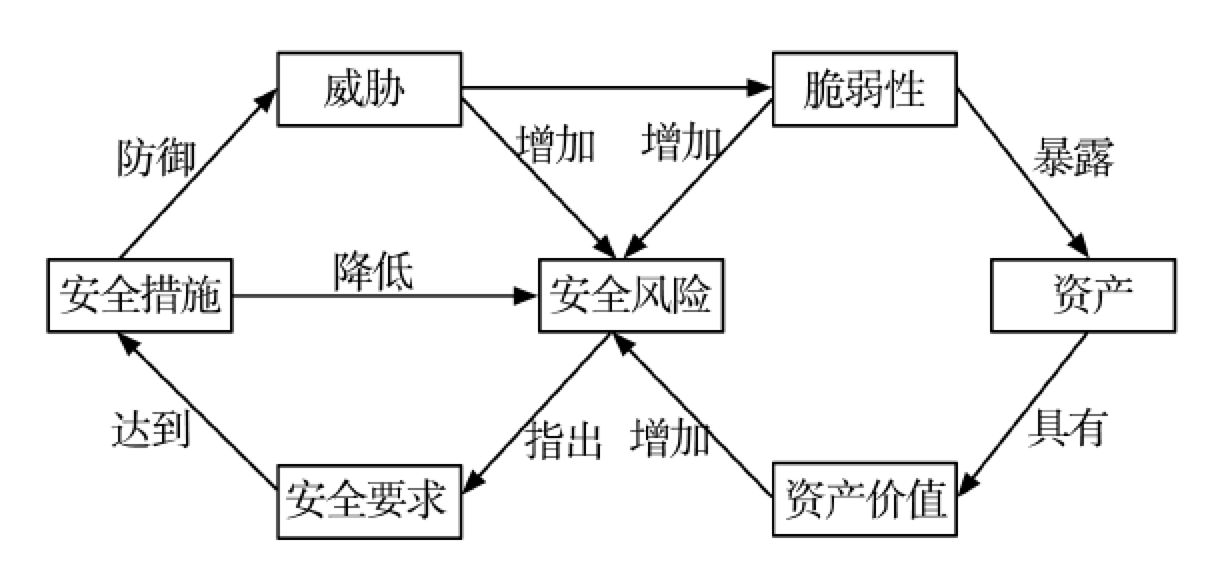


图 10-1 风险评估原理图

其基本思想参照 ISO 13335,该规范给实施信息安全管理者提出建议和指导。用户可以参照这个标准制定出自己的安全管理计划和实施方案。它对安全定义了 6 个特性:机密性、完整性、可用性、负责性、确实性和可靠性,使得风险评估考虑的问题更加完善。ISO 13335 的风险评估所考虑的主要因素同样包括:资产、威胁、脆弱性、影响、风险、安全措施和残余风险。

10.2 风险评估的国际标准

10.2.1 可信计算机系统评估准则(TCSEC)

TCSEC(Trusted Computer System Evaluation Criteria)标准是计算机系统安全评估的第一个正式标准,具有划时代的意义。该准则于 1970 年由美国国防科学委员会提出,并于 1985 年 12 月由美国国防部公布。TCSEC 最初只是军用标准,后来延至民用领域。

TCSEC 将计算机系统的安全划分为 4 大类、8 个级别。

- D 类(无保护级)。D 类安全等级只包括 D1 一个级别。D1 的安全等级最低。D1 系统只为文件和用户提供安全保护。D1 系统最普通的形式是本地操作系统,或者是一个完全没有保护的网络。
- C 类(自主保护等级)。该类安全等级能够提供审慎的保护,并为用户的行动和责任提供审计能力。C 类安全等级从低到高可划分为 C1 和 C2 两类。
- B 类(强制保护等级)。该类系统具有强制性保护功能,保护意味着如果用户没有与安全等级相连,系统就不会让用户存取对象。B 类系统中的主要数据结构必须携带



敏感标记；系统的开发者还应为TCB提供安全策略模型以及TCB规约；应提供证据证明访问监控器得到了正确的实施。B类安全等级从低到高可分为B1、B2和B3三级。

- A类（验证保护等级）。A类的安全级别最高。A类系统的特点是使用形式化的安全验证方法，保证系统的自主和强制安全控制措施能够有效地保护系统中存储和处理的秘密信息或其他敏感信息。系统提供丰富的文档信息用以证明TCB满足设计、开发及实现等各个方面的安全要求。该类安全等级从低到高分为A1级和超A1级。

10.2.2　信息技术安全评估标准（ITSEC）

ITSEC（Information Technology Security Evaluation Criteria）是欧洲多国安全评价方法的综合产物，应用领域为军队、政府和商业。该标准将安全概念分为功能与评估两部分。功能准则从F1～F10共分10级，F1～F5级对应于TCSEC的D到A，F6～F10级分别对应数据和程序的完整性、系统的可用性、数据通信的完整性、数据通信的保密性以及机密性和完整性的网络安全。

与TCSEC不同，ITSEC并不把保密措施直接与计算机功能相联系，而是只叙述技术安全的要求，把保密作为安全增强功能。另外，TCSEC把保密作为安全的重点，而ITSEC则把完整性、可用性与保密性作为同等重要的因素。ITSEC定义了从E0级（不满足品质）到E6级（形式化验证）的7个安全等级。对于每个系统，安全功能可分别定义。

10.2.3　信息技术安全通用评估准则（ISO IEC 15408）

为了能集中世界各国安全评估准则的优点，集合成能被广泛接受的信息技术评估准则，1993年6月，在英、美、加、法、德、荷六国的合作下，形成了《信息技术安全通用评估准则》，简称：CC（Common Criteria）。CC的2.0版本于1999年12月被ISO批准为国际标准，编号ISO IEC 15408。我国于2001年将CC作为国家标准，以编号GB/T 18336发布。

CC吸收了各先进国家对现代信息系统安全的经验和知识，对信息安全的研究与应用产生了深刻的影响。它分为三部分，第一部分介绍CC的基本概念和基本原理，第二部分提出安全功能要求，第三部分提出安全保证要求。

CC通过对安全保证的评估而划分安全等级，每一等级对保证功能的要求各不相同。安全等级增强对保证组件的数目或强度的要求也会增加。CC安全等级简称EAL（评估保证级），共分7级，安全等级由EAL1到EAL7逐渐提高。

10.2.4　系统安全工程能力成熟度模型（SSE-CMM）

国际上通常采用能力成熟度模型（Capability Maturity Model，CMM）来评估一个组织的工程能力。CMM模型认为，能力成熟度高的企业持续生产高质量产品的可能性很大，而工程风险则很小。系统安全工程能力成熟度模型（Systems Security Engineering Capability



Maturity Model,SSE-CMM)是 CMM 在系统安全工程这个具体领域应用而产生的一个分支,是美国国家安全局领导开发的,其最关注的是安全工程过程域,是以动态的观点来管理、控制系统中动态的风险、影响和脆弱性。

在 SSE-CMM 模型中,将各种系统安全工程任务抽象、划分为 11 个有明显特征的子任务(即过程域 PA)。这 11 个过程域又可划分为风险过程、工程过程和保证过程 3 类,这 3 类过程也被称作 SSE-CMM 的三大安全焦点。

在 SSE-CMM 的三大安全焦点中,风险过程的位置比较特殊。就其作用而言,风险过程为工程过程提供了基本的安全需求信息,同时也为安全工程的结果提供了有效的评估手段。根据模型,那些足以成为风险的事件由三个组成部分:威胁、系统脆弱性和事件造成的影响。一般而言,这三种因素必须全都存在才足以造成风险(风险值大于零)。模型中定义了四个风险过程域:PA02 评估影响、PA03 评估安全风险、PA04 评估威胁和 PA05 评估脆弱性。具体关系如图 10-2 所示。

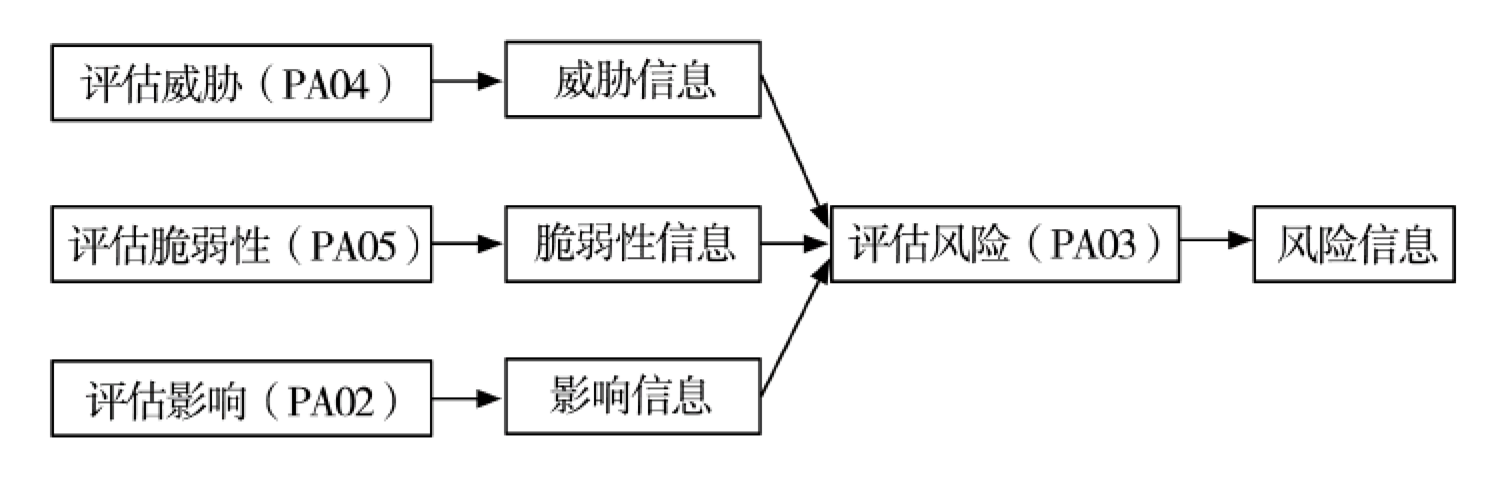


图 10-2　SSE-CMM 风险评估模型

首先,通过 PA02、PA04、PA05 这三个过程的具体实践分别得到系统的影响信息、威胁信息和脆弱性信息,然后利用 PA03 评估风险过程获得系统的风险信息。

目前,SSE-CMM 已经成为西方发达国家政府、军队和要害部门组织和实施安全工程的通用方法,是系统安全工程领域里成熟的方法体系。我国国家及军队信息安全测评认证中心已准备将 SSE-CMM 作为安全产品和信息系统安全性检测和认证的标准之一。

SSE-CMM 模型的能力等级由低到高分为五个级别。

10.3　风险评估分析方法

在风险评估和风险管理方法被应用的过程中,评估时间、力度以及具体开展的深度应与组织的环境和安全要求相称。按照风险评估的深度,风险评估方法可分为以下三类:基本的风险评估方法、详细的风险评估方法和联合的风险评估方法。

10.3.1　基本的风险评估方法

基本的风险评估是指应用直接和简易的方法达到基本的安全要求。这种方法适用于业务运作不是非常复杂的组织,并且组织对信息处理和网络的依赖程度不高的情况。

基本风险评估活动涉及的具体内容如下:

- 资产识别和估价。列出与信息安全管理体系范围内被评估的业务环境、运作和信息



相关的资产。

- 威胁评估。使用通用或常见的威胁列表，列出资产的威胁。
- 脆弱性评估。应用通用或常见的脆弱性列表，列出资产的脆弱性。
- 现有的和计划的安全控制的识别。根据前期的安全评审，对所有与资产相关联的现有的和计划的控制进行识别和文件化。
- 风险评估。收集由上述评估产生的有关资产、威胁和脆弱性的信息，进行一个系统的、简单的风险测量。
- 安全控制和降低风险的识别和选择。对于列出的每一项资产，确认与之相关的控制目标，选择适合的控制方法，完成各项安全控制任务。然后，评估被选择的安全控制多大程度上降低了被识别的风险。
- 风险接受。有可能需要采取进一步的控制措施来降低剩余风险。

基本风险评估简单易行，有较高的经济效益。但是，其安全程度的设置较难把握，如果信息安全管理体系升级，那么使用该方法将很难评估最初的控制是否仍然安全。

10.3.2　详细的风险评估方法

详细的风险评估包括资产的详细识别和估价，是非常耗费财力的完整的过程，因此需要非常仔细地确定被评估的信息系统的业务环境、运作、信息及资产的边界。它需要管理者持续关注。

详细风险评估活动涉及的具体内容如下：

- 资产识别和估价。识别和列出信息安全管理范围内被评估的业务环境、运作和信息相关的所有资产，定义一个价值尺度并为每一项资产分配价值（保密性、完整性和可用性的价值）。
- 威胁评估。识别与资产相关的所有威胁，并根据它们发生的可能性和严重性为它们赋值。
- 脆弱性评估。识别与资产相关的所有脆弱性，并根据它们被威胁利用的难易程度来为它们赋值。
- 现有的和计划的安全控制的识别。根据前期评审，将所有现有的和计划的与资产相关的安全控制进行识别和文件化。
- 风险评估。利用上述对资产、威胁、脆弱性的评价结果，进行风险计算，风险为资产的相对价值、威胁发生的可能性与薄弱点被利用的可能性的函数，采用适当的风险测量工具进行风险计算。
- 安全控制和降低风险的识别和选择。根据从上述评估中识别的风险，采取适当的安全控制方法，以阻止这些风险。然后，评估被选择的安全控制多大程度上降低了被识别的风险。
- 风险接受。对残余的风险加以分类，或是“可接受的”或是“不可接受的”。对那些被确认是“不可接受的”，决定选择更进一步的控制还是改变可接受风险的程度。

详细风险评估能获得一个更准确的安全风险认识，能更确切地反映组织对安全程度的要求。但是，它需要花费大量的时间、精力和技术，有可能提出的安全措施已滞后于时间



要求。

10.3.3 联合的风险评估方法

联合评估方法首先鉴定出一个信息系统中的高风险、关键、敏感部分，对其进行详细的风险评估分析，然后对其他的部分采取基本的风险评估分析。

联合评估方法综合了基本风险评估和详细风险评估方法的优点，在合理花费时间和精力的前提下，获得一个全面的系统评估结果，使宝贵的资源和资金能够用在最需要的地方。但是，如果对信息系统风险程度的高低判别不正确，可能导致错误的结果。比如，一个需要使用详细风险评估方法的系统，采用了基本的风险评估方法，造成不能精确地识别系统的风险，从而不能为系统制定最有效的安全措施。

10.4 风险评估的步骤

为了确定未来的不利事件发生的可能性，必须对信息系统面临的威胁、可能的脆弱性以及信息系统中部署的安全控制一起进行分析。风险评估方法包括以下七个步骤：风险评估准备、资产识别、威胁识别、脆弱性识别、已有安全措施确认、风险控制方案提出和评估报告形成，如图 10-3 所示。

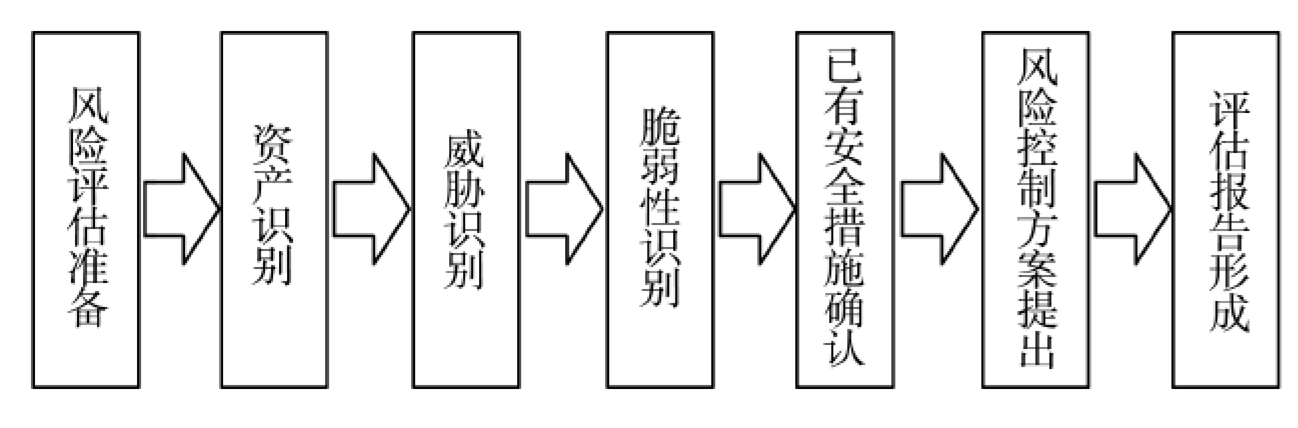


图 10-3　风险评估步骤

10.4.1 风险评估准备

风险评估的准备是实施风险评估的前提，只有有效地进行了信息安全风险评估准备，通过确定目标、进行调研、获得组织高层管理者对评估的支持等，才能更好地开展信息安全风险评估。

风险评估的准备活动包括：

- 确定风险评估的目标；
- 确定风险评估的范围；
- 组建评估管理团队和评估实施团队；
- 进行系统调研；
- 确定评估依据和方法；
- 获得最高管理者对风险评估工作的支持。

1. 风险评估目标的确定

信息安全需求是一个组织为保证其业务正常、有效运转而必须达到的信息安全要求，通过分析组织必须符合的相关法律法规，组织在业务流程中对信息安全等的机密性、可用性、完整性等方面的需求，来确定风险评估的目标。

2. 风险评估范围的确定

风险评估的范围包括组织内部与信息处理相关的各类软硬件资产、相关的管理机构和人员、所处理的信息等各方面。实施一次风险评估的范围可大可小，需要根据具体评估需求确定，可以对组织全部的信息系统进行评估，也可以仅对关键业务流程进行评估，也可以对组织的关键部门的信息系统进行评估等。本例只对计算机系统进行评估，评估范围如表 10-1 所示。

表 10-1　确定评估范围　　　　单位：台

资产名称	数量	资产名称	数量
主域控制器	1	Web 服务器	2
备份域控制器	1	DHCP 服务器	1
邮件服务器	2	DNS 服务器	1
FTP 服务器	1		

3. 系统调研

在确定了风险评估的目标、范围、团队后，要进行系统调研，并根据系统调研的结果决定评估将采取的评估方法等技术手段。系统调研内容包括：

- 组织业务战略；
- 管理制度；
- 组织主要业务功能和要求；
- 网络结构、网络环境（包括内部连接和外部连接）；
- 网络系统边界；
- 主要的硬件、软件；
- 数据和信息；
- 系统和数据的敏感性；
- 系统使用人员；
- 其他。

系统调研可以采取问卷调查、现场访谈等方法进行。

4. 风险评估方法确定

以系统调研结果为依据，根据被评估信息系统的具体情况，确定风险评估依据和方法。评估依据包括（但不限于）现有国际或国家有关信息安全标准、组织的行业主管机关的



业务系统的要求和制度、组织的信息系统互联单位的安全要求、组织的信息系统本身的实时性或性能要求等。

根据评估依据,并综合考虑评估的目的、范围、时间、效果、评估人员素质等因素,选择具体的风险方法,并依据组织业务实施对系统安全运行的需求,确定相关的评估判断依据,使之能够与组织环境和安全要求相适应。

10.4.2 资产识别

1. 资产定义

资产是企业、机构直接赋予了价值因而需要保护的东西。它可能是以多种形式存在,包括无形的、有形的、硬件、软件、文档、代码,还包括服务、企业形象等。

资产具有很强的时间特性,它的价值和安全属性都会随着时间的推移发生变化,所以应该根据时间变化的频度制定资产相关的评估和安全策略的频度。

2. 资产的识别和估价

为了明确被保护的信息资产,组织应列出与信息安全有关的资产清单,对每一项资产进行确认和适当的评估。

在列出所有信息资产后,应对每项资产赋予价值。对资产进行估价时,不仅要考虑资产的账面价格,更重要的是考虑资产对于组织的商务的重要性,即根据资产损失所引发的潜在的商务影响来决定。一些信息资产是有时效性的,例如,新产品数据在产品面市之前是高度机密的。采用精确的财务方式来给资产确定价值有时候很难,一般采用定性的方式来建立资产的价值或重要程度,即按照事先确定的价值尺度将资产的价值划分为不同等级。

经过资产识别与估价后,组织应根据资产价值的大小进一步确定需要保护的关键资产,如表 10-2 所示。

表 10-2 确定需要保护的关键资产 单位:元

资产名称	物理价值	软件名称	破坏影响	资产价值
主域控制器	18 000	Windows	全部业务停止	35 000
备份域控制器	18 000	Windows	全部业务停止	35 000
邮件服务器 A	22 000	Exchange	全部业务停止	42 000
邮件服务器 B	22 000	Exchange	全部业务停止	42 000
FTP 服务器	10 000	IIS	大部分业务停止	20 000
Web 服务器 A	12 000	IIS	大部分业务停止	18 000
Web 服务器 B	12 000	IIS	大部分业务停止	18 000
DHCP 服务器	10 000	Windows	大部分业务停止	20 000
DNS 服务器	10 000	Windows	大部分业务停止	20 000



10.4.3　威胁识别

1. 威胁定义

安全威胁是对机构及其资产构成潜在破坏的可能性因素或者事件。无论对于多么安全的信息系统,安全威胁是一个客观存在的事物,它是风险评估的重要因素之一。

2. 威胁的识别与评估

对组织需要保护的每一项关键资产进行威胁识别时,应根据资产所处的环境条件和资产以前遭受威胁损害的情况来判断,一项资产可能面临着多个威胁。同样,一个威胁可能对不同的资产造成影响。威胁识别应确认威胁由谁或什么事物引发以及威胁影响的资产。用于威胁评估的信息可以从信息安全管理的有关人员,以及相关的商业过程中获得,这些人可能是人事部的职员、设备策划和 IT 专家,也包括组织内部负责安全的人员。

确定威胁发生的可能性是风险评估的重要环节,组织应根据经验和有关的统计数据来判断威胁发生的频率或者发生的概率。根据威胁发生的可能性给予假设值,如表 10-3 所示。

表 10-3　确定威胁发生的可能性　　单位:%

威　　胁	发生可能性	威　　胁	发生可能性
断电	75	网络故障	55
病毒	70	雷电	10
硬件故障	65	地震	0.01
内部攻击	10	水灾	0.01
外部攻击	50	火灾	1

10.4.4　脆弱性识别

1. 脆弱性定义

脆弱性是资产本身存在的,它可以被威胁利用,引起资产或商业目标的损害。脆弱性包括物理环境、机构、过程、人员、管理、配置、硬件、软件和信息等各种资产的脆弱性。

2. 脆弱性识别与评估

脆弱性识别是风险评估中最重要的一个环节。脆弱性识别可以以资产为核心,针对每一项需要保护的资产,识别可能被威胁利用的弱点,并对脆弱性的严重程度进行评估;也可以从物理、网络、系统、应用等层次进行识别,然后与资产、威胁对应起来。表 10-4 提供了一种脆弱性识别内容的参考。



表 10-4 脆弱性识别内容表

类型	识别对象	识别内容
技术脆弱性	物理环境	从机房场地、机房防火、机房供配电、机房防静电、机房接地与防雷、电磁防护、通信线路的保护、机房区域防护、机房设备管理等方面进行识别
	网络结构	从网络结构设计、边界保护、外部访问控制策略、内部访问控制策略、网络设备安全配置等方面进行识别
	系统软件(含操作系统及系统服务)	从补丁安装、物理保护、用户账号、口令策略、资源共享、事件审计、访问控制、新系统配置(初始化)、注册表加固等方面进行识别
	数据库软件	从补丁安装、鉴别机制、口令机制、访问控制、网络和服务设置、备份恢复机制、审计机制等方面进行识别
	应用中间件	从协议安全、交易完整性、数据完整性等方面进行识别
	应用系统	从审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密码保护等方面进行识别
管理脆弱性	技术管理	从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别
	组织管理	从安全策略、组织安全、资产分类与控制、人员安全、符合性等方面进行识别

通常而言,脆弱性评估包括漏洞评估、手工评估、自动评估、渗透测试等方面。

- 漏洞评估指通过扫描器对操作系统、网络设备等进行评估;
- 手工评估指通过人工手动评价已知的安全漏洞;
- 自动评估指通过硬件和软件设备自动定期或者非定期对网络、系统进行评估;
- 渗透测试指在系统不进行任何改变的情况下,从外界模拟真实攻击的方式,对系统进行评估。

10.4.5 已有安全措施确认

安全措施可以分为预防性安全措施和保护性安全措施两种。预防性安全措施可以降低威胁利用脆弱性导致安全事件发生的可能性,如入侵检测系统;保护性安全措施可以减少因安全事件发生后对组织或系统造成的影响。

在识别脆弱性的同时,评估人员应对已采取的安全措施的有效性进行检查,检查安全措施是否有效发挥了作用,即是否真正地降低了系统的脆弱性,抵御了威胁。对于已经有效地发挥了其作用的安全措施,应继续保持,而不用重复建设安全措施;对于不适当的安全措施,应对其进行改进,或采用更合适的安全措施替代。

10.4.6 风险控制方案提出

在这一步里,对不可接受的风险应根据导致该风险的脆弱性制定一个风险控制方案,该方案的目标是减缓或消除已识别的风险,降低系统的风险级别,使其达到一个可接受的水平。方案中应明确指出采取的弥补措施、预期效果、实施条件、进度安排、责任部门等。安全



措施的选择应从管理与技术两个方面考虑，管理措施作为技术措施的补充。

在提出控制方案时，应该考虑下列因素：

方案的有效性（如系统的兼容性）；

- 法律法规；
- 机构策略；
- 运行影响；
- 安全性和可靠性。

风险控制方案是风险评估过程的结果，在此后的风险减缓过程中，所提出的流程和技术类安全控制将得到评估并实现。但并不是所有的控制项目都能实现并降低损失，针对具体的系统，要确定哪些控制项目是适合的，要作实施成本分析，使得这些控制项目实施在成本上是可行的。另外，在风险减缓过程中，对实施该方案所带来的运行影响（例如对系统性能的影响）和可行性（例如技术要求、用户的接受程度）等方面也要仔细评估。

10.4.7　评估报告形成

当威胁源和系统脆弱性被识别出来，风险得到评估，风险控制方案也提出，风险评估即全部结束，该过程的结果将被记录到评估报告里。

风险评估报告是一份管理报告，它描述了系统面临的威胁和脆弱性及其风险度量，为风险控制的实现提供了依据。它可以帮助高级管理人员对策略、流程、预算以及系统的运行和管理变更等做出决策。不同于审计或调查报告（目的是为了检查错误），风险评估报告是以一种系统和分析的方法来评估风险，这样高级管理人员才能理解风险并为降低和修正可能出现的损失而分配资源。

10.5　习　　题

1. 简述 TCSEC 的安全级别。
2. ITSEC 比 TCSEC 有哪些进步？
3. 简述 CC 的安全级别。
4. 风险评估分析方法分为哪几类？各有什么特点？
5. 简述风险评估的步骤。

参 考 文 献

[1] 王达.网管员必读：网络安全.北京：电子工业出版社,2007
[2] 王文寿,王珂.网管员必备宝典——Windows Server 2003 网络管理.北京：清华大学出版社,2007
[3] 王常吉,龙冬阳.信息与网络安全实验教程. 北京：清华大学出版社,2007
[4] 王隆杰,梁广民等. Windows Server 2003 网络管理实训教程. 北京：清华大学出版社,2006
[5] 刘远生等.计算机网络安全.北京：清华大学出版社,2006
[6] 戴英侠等.计算机网络安全. 北京：清华大学出版社,2005
[7] 印润远.计算机信息安全.北京：铁道出版社,2006
[8] 刘宁等.计算机网络技术.北京：电子工业出版社,2006
[9] 戴有炜.ISA Server 2006 防火墙安装与管理指南.北京：北京科海电子出版社,2008
[10] 刘建伟等.网络安全实验教程.北京：清华大学出版社,2007
[11] 刘宁等.计算机网络实验与实训.北京：电子工业出版社,2006